Norton™ Personal Firewall User's Guide

Norton™
Personal Firewall 2002

Norton™ Personal Firewall User's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 4.0

PN: 07-30-00468

Copyright Notice

Copyright © 2001 Symantec Corporation. All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Standard Template Library

This product utilizes the Standard Template Library, a C++ library of container classes, algorithms, and iterators.

Copyright © 1996-1999. Silicon Graphics Computer Systems, Inc.

Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Silicon Graphics makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Copyright © 1994. Hewlett-Packard Company

Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Hewlett-Packard Company makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Trademarks

Symantec, the Symantec logo, Norton, Norton Internet Security, Norton Personal Firewall, Norton SystemWorks, Emergency Disk, LiveUpdate, Norton AntiVirus, Norton Utilities, and Rescue Disk are trademarks of Symantec Corporation.

Windows is a registered trademark of Microsoft Corporation. AOL and CompuServe are registered trademarks of America Online, Inc. Prodigy Internet is a trademark of Prodigy. Pentium is a registered trademark of Intel Corporation.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC LICENSE AND WARRANTY

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHER USE OF THE SOFTWARE, AND RETURN THE FULL PRODUCT WITH PROOF OF PURCHASE TO THE DEALER FROM WHOM IT WAS ACQUIRED WITHIN SIXTY (60) DAYS OF PURCHASE, AND YOUR MONEY WILL BE REFUNDED.

1. License.

The software which accompanies this license (collectively the "Software") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that Symantec may furnish to you. Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") which accompanies, precedes, or follows this license, your rights and obligations with respect to the use of this Software are as follows:

You may:

A. use one copy of the Software on a single computer. If a License Module accompanies, precedes, or follows this license, you may make that number of copies of the Software licensed to you by Symantec as provided in your License Module. Your License Module shall constitute proof of your right to make such copies.

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of your computer and retain the original for archival purposes;

C. use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network; and

D. after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this license.

You may not:

A. copy the printed documentation which accompanies the Software;

B. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

D. use a later version of the Software than is provided herewith unless you have purchased upgrade insurance or have otherwise separately acquired the right to use such later version;

E. use, if you received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which you have not received a permission in a License Module; or

F. use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Symantec software products utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for any period for which you have purchased a subscription for Content Updates for the Software (including any subscription included with your original purchase of the Software), purchased upgrade insurance for the Software, entered into a maintenance agreement that includes Content Updates, or otherwise separately acquired the right to obtain Content Updates. This license does not otherwise permit you to obtain and use Content Updates.

3. Sixty Day Money Back Guarantee:

If you are the original licensee of this copy of the Software and are dissatisfied with it for any reason, you may return the complete product, together with your receipt, to Symantec or an authorized dealer, postage prepaid, for a full refund at any time during the sixty (60) day period following the delivery to you of the Software.

4. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

5. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR

INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

6. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are “Commercial Items”, as that term is defined in 48 C.F.R. section 2.101, consisting of “Commercial Computer Software” and “Commercial Computer Software Documentation”, as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec’s computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement may only be modified by a License Module or by a written document which has been signed by both You and Symantec. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write: (i) Symantec Customer Service, 175 W. Broadway, Eugene, OR 97401, USA, or (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland.

This product utilizes the Standard Template Library, a C++ library of container classes, algorithms, and iterators. Copyright © 1996-1999. Silicon Graphics Computer Systems, Inc. Copyright © 1994. Hewlett-Packard Company.

How to minimize Internet risks

Install Norton Personal Firewall.

For more information, see "Installing Norton Personal Firewall" on page 17.

Run LiveUpdate weekly to keep protection current.

For more information, see "Getting started with Norton Personal Firewall" on page 29.

Identify private information to safeguard.

For more information, see "Protecting confidential information" on page 43.

Respond appropriately to Norton Personal Firewall alerts.

For more information, see "Responding to Norton Personal Firewall alerts" on page 49.

Customize firewall protection.

For more information, see "Customizing firewall protection" on page 61.

Keep Norton Personal Firewall protection enabled.

For more information, see "Customizing firewall protection" on page 61.

C O N T E N T S

How to minimize Internet risks

Chapter 1 Introducing Norton Personal Firewall

Preventing unauthorized access 13
Protecting personal information 15
Online assistance 15
Tips for safe computing 16

Chapter 2 Installing Norton Personal Firewall

System requirements 17
- Windows 98/Me 17
- Windows NT 4.0 Workstation 18
- Windows 2000 Professional Workstation 18
- Windows XP Home Edition/Professional 18

Before installation 18
Installation 19
- If the opening screen does not appear 22

Registering your software 23
After installation 24
- Restarting your computer 24
- Using the Information Wizard 24
- Using the Security Assistant 25

If you have Norton SystemWorks installed 26
If you need to uninstall Norton Personal Firewall 26

Chapter 3 Getting started with Norton Personal Firewall

Starting Norton Personal Firewall 29
Temporarily disabling Norton Personal Firewall 30
- Disabling a protection feature 31

Keeping current with LiveUpdate 31
- About program updates 31
- About protection updates 32
- About your subscription 32
- Obtain program and protection updates 32

Getting help with Norton Personal Firewall 33
Comprehensive online Help 33
Window and dialog box Help 33
What's This? Help for buttons and other controls 33
Readme file and Release Notes 34
Using the Security Assistant 35
Personal Firewall 35
Privacy Control 36
Application Control 38
Internet Zone Control 39
Internet Status 40
Alert Tracker 40
LiveUpdate 40
Running Security Check 41

Chapter 4 Protecting confidential information

Setting the Privacy Level 44
Adding confidential information to be blocked 44
Adjusting privacy settings 45
Changing the Confidential Information setting 46
Changing the Cookie Blocking setting 46
Enabling Browser Privacy 47
Enabling secure Web connections 47
Blocking secure Web connections 47

Chapter 5 Responding to Norton Personal Firewall alerts

Responding to Security Alerts 50
Responding to Internet Access Control alerts 52
Responding to Java and ActiveX Alerts 54
Responding to Cookie Alerts 55
Responding to Confidential Information Alerts 56
Using Alert Tracker 57
Opening Alert Tracker 57
Reviewing recent Alert Tracker messages 58
Moving Alert Tracker 58
Hiding Alert Tracker 58
Adjusting the reporting detail 58
Setting the Reporting Level 59

Chapter 6 Customizing firewall protection

Setting the Security Level 62
Making custom security settings 63
Controlling applications that access the Internet 66
Scanning for Internet-enabled applications 67
Enabling Automatic Internet Access Control 67
Responding to Internet Access Control alerts 67
Adding an application to Internet Access Control 68
Changing Internet Access Control settings 68
Changing system-wide settings 69
Home network control with Internet Zone Control 69
Adding computers to zones 70
Adding computers on your home network to the Trusted zone 70
Using Intrusion Protection to stop attacks 72
Detecting Port Scan Attempts 72
Enabling AutoBlock 72
Unblocking a blocked computer 73
Excluding specific activities from AutoBlock 73
Restricting a blocked computer 74
Identifying computers to Norton Personal Firewall 74
Specifying individual computers 75
Specifying a range of computers 75
Specifying computers using a network address 76

Chapter 7 Monitoring Norton Personal Firewall events

Reviewing Current Status 77
Checking Personal Firewall status 78
Checking Privacy status 78

Chapter 8 Configuring Norton Personal Firewall for common situations

Using Norton Personal Firewall with a dial-up connection 79
Using Norton Personal Firewall with a broadband connection 79
Troubleshooting broadband problems 80
Using Norton Personal Firewall with multiplayer games 81
Giving a multiplayer game access to the Internet 81
Placing other players in the Trusted zone 81
Using Norton Personal Firewall on a home network 82
Enabling file and printer sharing 82
Internet connection sharing 83

Using Norton Personal Firewall with a cable or DSL router 83
Using Norton Personal Firewall on a corporate network 83
Enabling file and printer sharing 84
Administrative software on corporate networks 84
Using Norton Personal Firewall with a proxy server 84
Determining whether Norton Personal Firewall works with your proxy server 84
Determining which port to monitor for HTTP communication 85
Specifying which ports to monitor for HTTP communication 86
Running a Web server with Norton Personal Firewall 86
Running an FTP server with Norton Personal Firewall 87
Using Norton Personal Firewall with DHCP 87
Using Norton Personal Firewall with pcAnywhere 88
Using Norton Personal Firewall with a VPN 88

Chapter 9 Troubleshooting

Troubleshooting Norton Personal Firewall problems 89
What is wrong with this Web site? 89
Why can't I post information online? 91
Why doesn't Norton Personal Firewall notify me before letting applications access the Internet? 91
Why doesn't my local network work? 92
Why can't I print to a shared printer? 92
How can a Web site get my browser information? 92

Appendix A About the Internet

How information is transmitted over the Internet 94
TCP/IP 95
UDP 95
ICMP 96
IGMP 96
Web information is located on the Internet 96
Requesting a page 97
Parts of a URL 97
Ports identify applications on a server 98
How computers are identified on the Internet 100

Appendix B Understanding Internet risks

Risks from hackers 101
The process of a hacker attack 102
Risks from active content 104
Risks to your privacy 105
Sending confidential information 105
Good cookies and bad cookies 105
Tracking Internet use 106
Risks from Trojan horses and viruses 107
The likelihood of being attacked 108

Service and support solutions

CD Replacement Form

Index

CHAPTER 1

Introducing Norton Personal Firewall

Millions of computers connect to the Internet, and the number increases daily. When you are connected to the Internet, you can connect with millions of other computers and those computers can connect with your computer. Unprotected connections to the Internet leave your computer vulnerable to hacker attacks and other Internet threats.

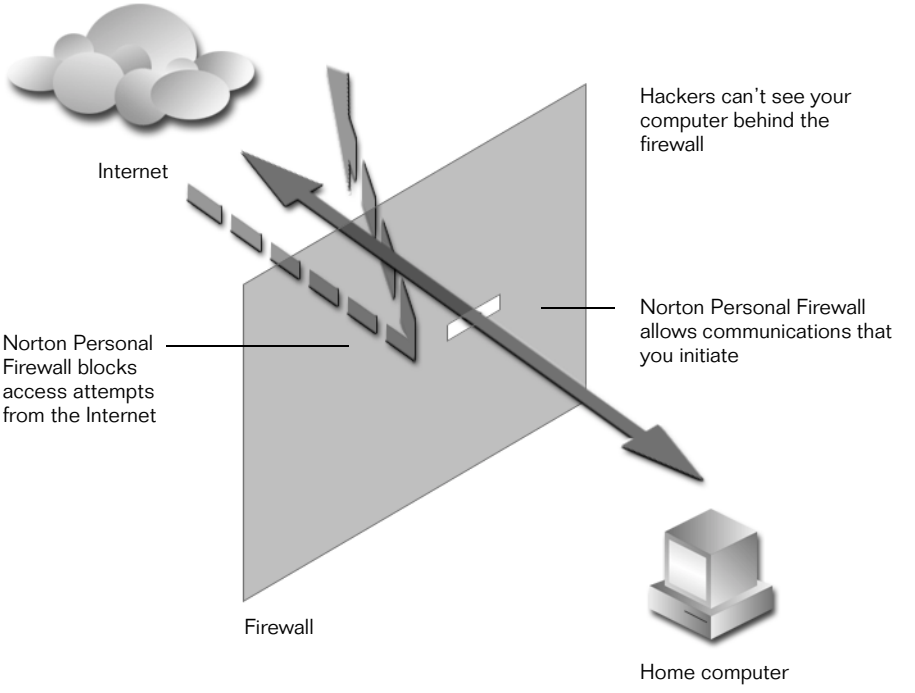
Norton Personal Firewall includes several components that work together to protect you from Internet threats and enhance your Internet experience in the following ways:

- Prevents unauthorized access to your computer when you are on the Internet
- Protects your personal information

Preventing unauthorized access

Norton Personal Firewall provides a barrier between your computer and the Internet. A *firewall* prevents unauthorized access to or from a computer or network. Firewalls prevent unauthorized Internet users from accessing private computers and networks connected to the Internet.

Norton Personal Firewall uses rules to determine whether to permit or block connections. You can change these rules, permitting or blocking applications from having Internet access.


Internet
Hackers can't see your computer behind the firewall
Norton Personal Firewall allows communications that you initiate
Norton Personal Firewall blocks access attempts from the Internet
Firewall
Home computer

Norton Personal Firewall can automatically determine the best way to protect many applications. When an application that Norton Personal Firewall does not recognize attempts to communicate over the Internet, Norton Personal Firewall alerts you, and helps you determine if Internet access is appropriate for that application.

ActiveX controls and *Java applets* are applications that run in your browser. While most of these applications are useful, some are harmful. Norton Personal Firewall can be configured to prevent ActiveX controls and Java applets from running without your knowledge, and lets you specify sites on which these applications can run.

Protecting personal information

You may not want confidential information, such as credit card numbers or your home phone number, to be sent unencrypted over the Internet. Privacy Control prevents confidential information from being sent over nonsecure connections to Web sites or through instant messenger programs.

Cookies are small files stored on your computer that Web sites use to track your Web usage. Norton Personal Firewall can block cookies and other information that your browser normally reports to Web sites, such as the address of the previous Web site that you visited and the type of Web browser you are using.

Online assistance

Norton Personal Firewall provides extensive online assistance.

- The Security Assistant is a wizard that introduces you to Norton Personal Firewall and helps you select the correct settings to maximize your protection. After you install Norton Personal Firewall and restart your computer, the Security Assistant appears. The Security Assistant is always available to provide information about how Norton Personal Firewall works, or to change any of the settings you selected.
- Online Help is a comprehensive reference to Norton Personal Firewall. It includes a table of contents, a comprehensive index, and full-text search capabilities, making it easy to find the information you need.
- In most windows and dialog boxes, Tell Me More or Help is available to provide specific information about where you are in Norton Personal Firewall.
- What's This? Help provides a quick definition of an individual component of a window or dialog box.

Tips for safe computing

Norton Personal Firewall provides many of the tools you need to minimize Internet risks. Other things you can do to ensure safe Internet use include:

- Keep your browser up-to-date. Software publishers release new versions to fix vulnerabilities that have been found in their browsers.
- Use passwords intelligently. For important information, use complex passwords that include capital and lowercase letters, numbers, and symbols. Don't use the same password in multiple places.
- Don't run software if you don't trust the publisher and the source from which you received the software.
- Don't open email attachments unless you are expecting the attachment and you trust the sender.
- Be sensible about providing personal information where it isn't warranted. Many sites ask for more information than they need.
- Review the privacy policies of the sites to which you are considering sending information.

For more information, see "Understanding Internet risks" on page 101.

CHAPTER 2

Installing Norton Personal Firewall

Before installing Norton Personal Firewall, take a moment to review the system requirements listed in this chapter.

System requirements

To use Norton Personal Firewall, your computer must have one of the following Windows operating systems:

- Windows 98, 98SE
- Windows Me
- Windows NT v4.0 Workstation operating system with Service Pack 6a or higher
- Windows 2000 Professional Workstation
- Windows XP Professional or Windows XP Home Edition

Your computer must also meet the following minimum requirements.

Windows 98/Me

- Intel Pentium processor at 150 MHz
- 32 MB of RAM
- 20 MB of available hard disk space
- Internet Explorer 4.01 Service Pack 1 or higher
- CD-ROM or DVD-ROM drive
- Microsoft Windows Internet support

Windows NT 4.0 Workstation

- Service Pack 6a or higher
- Intel Pentium processor at 150 MHz
- 48 MB of RAM
- 20 MB of available hard disk space
- Internet Explorer 4.01 Service Pack 1 or higher
- CD-ROM or DVD-ROM drive
- Microsoft Windows Internet support

Windows 2000 Professional Workstation

- Intel Pentium processor at 150 MHz
- 48 MB of RAM
- 20 MB of available hard disk space
- Internet Explorer 4.01 Service Pack 1 or higher
- CD-ROM or DVD-ROM drive
- Microsoft Windows Internet support

Windows XP Home Edition/Professional

- Intel Pentium processor at 300 MHz or higher
- 64 MB of RAM
- 20 MB of available hard disk space
- Internet Explorer 4.01 Service Pack 1 or higher
- CD-ROM or DVD-ROM drive
- Microsoft Windows Internet support

Before installation

If you have previous versions of Norton Personal Firewall or any other firewall programs on your computer, you must uninstall them before installing this version of Norton Personal Firewall. For more information, see "If you need to uninstall Norton Personal Firewall" on page 26.

To uninstall other firewall programs, see the user documentation that came with the program.

You must also quit all other Windows programs before installing Norton Personal Firewall.

If you are using Windows XP, disable the XP firewall.

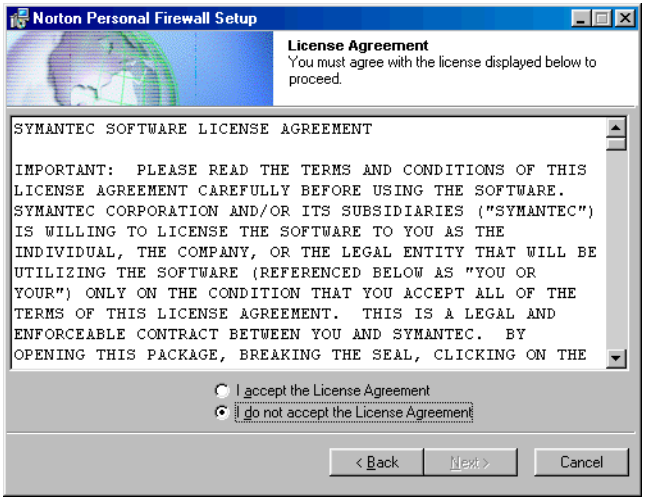
Installation

Install Norton Personal Firewall from the Norton Personal Firewall CD.

To install Norton Personal Firewall

1. Insert the Norton Personal Firewall CD into the CD-ROM drive.
2. In the Norton Personal Firewall CD window, click **Install Norton Personal Firewall**.

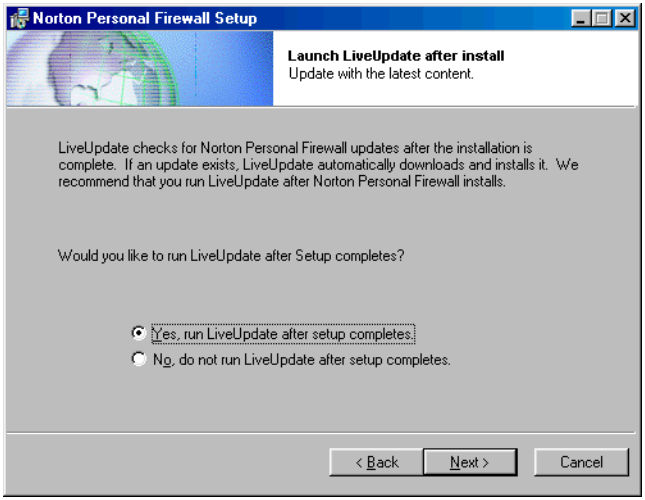
   If your computer is not set to automatically open a CD, you will have to open it yourself. For more information, see "If the opening screen does not appear" on page 22.
3. The first installation window reminds you to close all other Windows programs. Click **Next**.


Norton Personal Firewall Setup
License Agreement
You must agree with the license displayed below to proceed.
SYMANTEC SOFTWARE LICENSE AGREEMENT
IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE
I accept the License Agreement
I do not accept the License Agreement
< Back
Next >
Cancel

4. In the License Agreement window, click **I accept the License Agreement**.

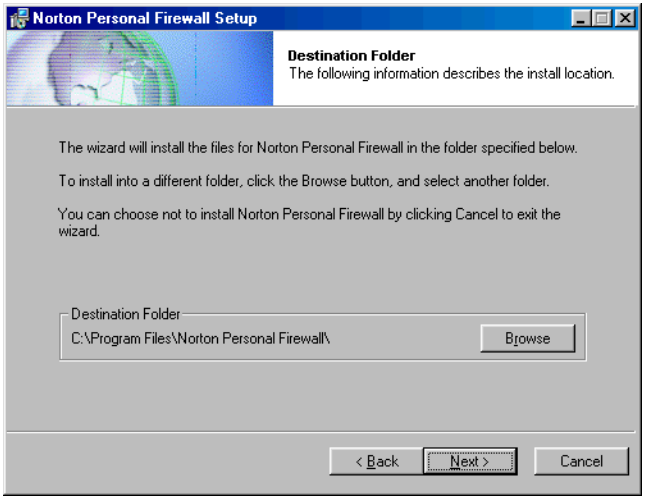
   If you decline, you cannot continue with the installation.

5 Click **Next**.


Norton Personal Firewall Setup
Launch LiveUpdate after install
Update with the latest content.
LiveUpdate checks for Norton Personal Firewall updates after the installation is complete. If an update exists, LiveUpdate automatically downloads and installs it. We recommend that you run LiveUpdate after Norton Personal Firewall installs.
Would you like to run LiveUpdate after Setup completes?
Yes, run LiveUpdate after setup completes.
No, do not run LiveUpdate after setup completes.
< Back
Next >
Cancel

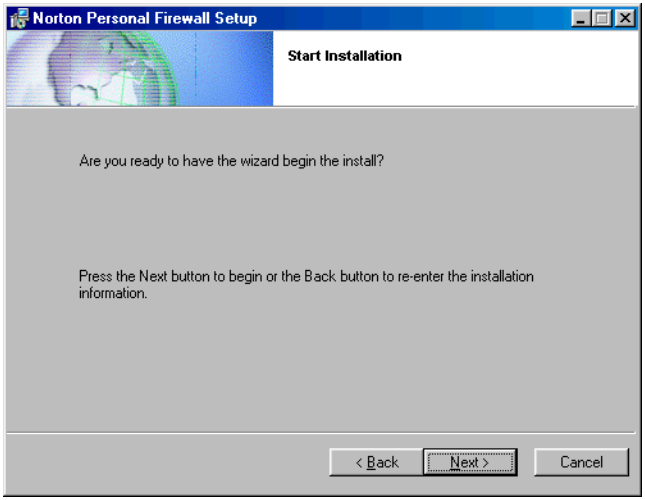
6 LiveUpdate keeps your copy of Norton Personal Firewall up to date with the latest program and protection updates. Select whether or not you want to run LiveUpdate after installation is done.

7 Click **Next**.

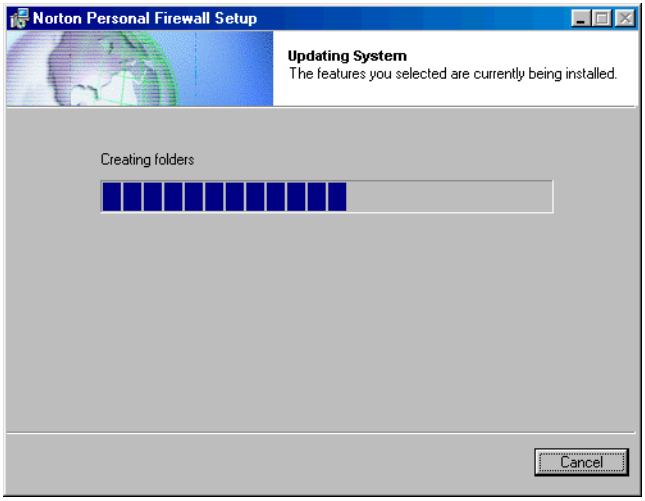

Norton Personal Firewall Setup
Destination Folder
The following information describes the install location.
The wizard will install the files for Norton Personal Firewall in the folder specified below.
To install into a different folder, click the Browse button, and select another folder.
You can choose not to install Norton Personal Firewall by clicking Cancel to exit the wizard.
Destination Folder
C:\Program Files\Norton Personal Firewall\
Browse
< Back
Next >
Cancel

8 Click **Browse** to select a folder into which you want Norton Personal Firewall installed, if other than the default location.

9 Click **Next**.


Norton Personal Firewall Setup
Start Installation
Are you ready to have the wizard begin the install?
Press the Next button to begin or the Back button to re-enter the installation information.
< Back
Next >
Cancel

10 Click **Next** to begin installing Norton Personal Firewall.



After Norton Personal Firewall is installed, the Registration Wizard appears with which you can register your software. For more information, see "Registering your software" on page 23.

If you chose to run LiveUpdate after installation, it runs after registration.

11 When LiveUpdate is done, click **Finish**.

12 Scroll through the Readme text, then click **Next**.

13 Click **Finish** to exit the installation.

If the opening screen does not appear

Sometimes, a computer's CD-ROM drive does not automatically start a CD.

To start the installation from the Norton Personal Firewall CD

1 On your desktop, double-click **My Computer**.

2 In the My Computer dialog box, double-click the icon for your CD-ROM drive.

3 From the list of files, double-click **CDSTART.EXE**.

Registering your software

Use the Registration Wizard to register your software online. If you skip online registration, you can register your software later using the Product Registration option on the Help menu.

To register your software

1. In the first Registration window, select the country from which you are registering and the country in which you live (if different), then click **Next**.
2. If you would like information from Symantec about Norton Personal Firewall, select the method by which you want to receive that information, then click **Next**.
3. Type your name and whether you want Norton Personal Firewall registered to you or your company, then click **Next**.
4. Type your address, then click **Next**.
5. Do one of the following:
   - Answer the survey questions to help Symantec improve its products and services, then click **Next**.
   - Skip the survey by clicking **Next**.
6. Select whether you want to register Norton Personal Firewall through the Internet or by mail.
   - If you want to register by mail, your computer must be connected to a printer that the Registration Wizard can use to print the registration form.
   - If you want to register using the Internet, you must be connected to the Internet.
7. Click **Next**.

   If you submitted your registration through the Internet, the Registration Wizard displays the serial number for your product.
8. Write down the serial number or click **Print** to get a copy of your registration information for future reference.
9. Click **Next**.
10. Select whether you want to use your existing profile the next time you register a Symantec product, or type the information as part of registration.
11. Click **Finish**.

After installation

If your computer needs to be restarted after Norton Personal Firewall is installed, a prompt appears giving you the option to do so immediately. After restart or, if your computer does not need to be restarted, after installation is complete, the Information Wizard appears. After you complete the Information Wizard, the Security Assistant appears to walk you through the configuration of Norton Personal Firewall.

Note: If you bought your computer with Norton Personal Firewall already installed, the Information Wizard appears the first time you start the product. You must accept the license agreement that appears in the Information Wizard for Norton Personal Firewall to be activated.

Restarting your computer

After installation, you may receive a prompt telling you that your computer needs to be restarted for the updates to take effect.

To restart your computer

- In the Installer Information dialog box, click **Yes**.

  If you click No, configuration of Norton Personal Firewall is not complete until you restart your computer.

Using the Information Wizard

The Information Wizard gives you information about the Symantec subscription service.

To use the Information Wizard

1. On the Welcome screen, click **Next**.

   If you purchased your computer with Norton Personal Firewall already installed, you must accept the license agreement in order to use Norton Personal Firewall. You can then register your software.

2. Click **I accept the license agreement**, then click **Next**.

   The Registration Wizard appears, with which you can register online. For more information, see "Registering your software" on page 23.

   When you have completed registration, information about your subscription appears.

3 Review the subscription service information, then click **Next**.

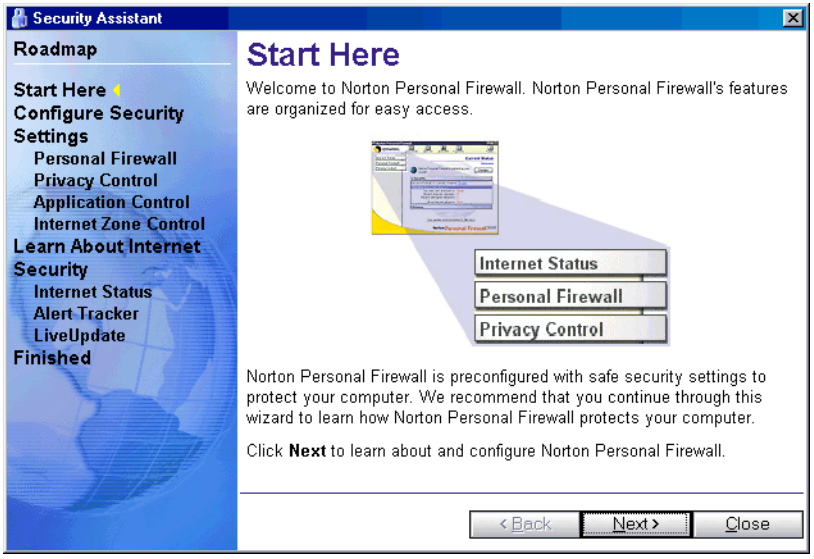
If you purchased your computer with Norton Personal Firewall already installed, the Readme file appears.

4 Scroll through the Readme, then click **Next**.

5 On the final Information Wizard screen, click **Finish**.

Using the Security Assistant

The Security Assistant begins automatically after you have completed the Information Wizard. You can use it to review and, if desired, change how Norton Personal Firewall has been configured for your computer.


Security Assistant
Roadmap
Start Here
Configure Security Settings
Personal Firewall
Privacy Control
Application Control
Internet Zone Control
Learn About Internet Security
Internet Status
Alert Tracker
LiveUpdate
Finished
Start Here
Welcome to Norton Personal Firewall. Norton Personal Firewall's features are organized for easy access.
Internet Status
Personal Firewall
Privacy Control
Norton Personal Firewall is preconfigured with safe security settings to protect your computer. We recommend that you continue through this wizard to learn how Norton Personal Firewall protects your computer.
Click Next to learn about and configure Norton Personal Firewall.
< Back
Next >
Close

Note: It is recommended that you use the default settings for Norton Personal Firewall. If you discover that changes need to be made after you have worked with Norton Personal Firewall for a while, you can use the Security Assistant to make those changes. For more information, see "Using the Security Assistant" on page 35.

To use the Security Assistant

- At the bottom of each pane, click **Next** to progress through the Security Assistant and review all settings.
- In the Roadmap on the left side of the Security Assistant window, click the name of a feature to review the settings for that feature.
- Click **Close** to close the Security Assistant.

If you have Norton SystemWorks installed

If you have Norton SystemWorks installed on your computer when you install Norton Personal Firewall, after you step through the Information Wizard you are asked if you want to integrate Norton Personal Firewall with Norton SystemWorks. If you click Yes, three things happen:

- A Norton Personal Firewall tab appears in the Norton SystemWorks main window. All Norton Personal Firewall features appear when you click the tab.
- Norton Personal Firewall appears as a tool in the Norton Tray Manager.
- If you attempt to open Norton Personal Firewall, Norton SystemWorks opens instead.

If you need to uninstall Norton Personal Firewall

If you need to remove Norton Personal Firewall from your computer, use Add/Remove Programs in the Windows Control Panel.

Note: During uninstall, Windows may indicate that it is installing software. This is a general Microsoft installer message and can be disregarded.

To uninstall Norton Personal Firewall

1. Do one of the following:
   - On the Windows taskbar, click **Start > Settings > Control Panel**.
   - On the Windows XP taskbar, click **Start > Control Panel**.
2. In the Control Panel, double-click **Add/Remove Programs**.
3. In the list of currently installed programs, click **Norton Personal Firewall**.
4. Do one of the following:
   - In Windows 2000 or Windows Me, click **Change/Remove**.
   - In Windows 98 or Windows NT, click **Add/Remove**.
   - In Windows XP, click **Remove**.
5. Click **Yes** to confirm that you want to uninstall the product.

If you have no other Symantec products on your computer, you should also uninstall LiveReg and LiveUpdate. Repeat steps 1 through 5 twice, first selecting LiveReg in step 3 to uninstall LiveReg, then select LiveUpdate in step 3 to uninstall LiveUpdate.

CHAPTER 3

Getting started with Norton Personal Firewall

Norton Personal Firewall starts automatically when you restart your computer. You do not have to open the program to be protected.

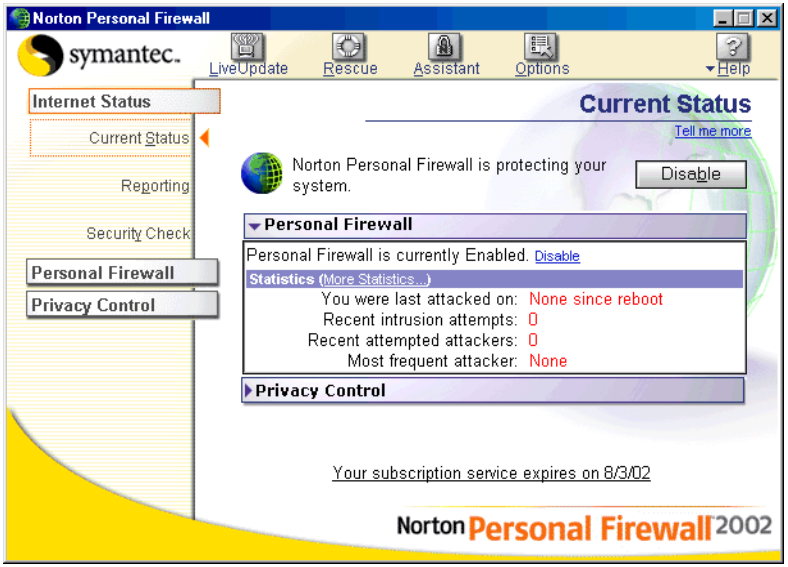
Starting Norton Personal Firewall

Start Norton Personal Firewall if you want to change protection settings or monitor the activities of the program.

To start Norton Personal Firewall

- Do one of the following:
  - In the notification area of the Windows taskbar, double-click **Norton Personal Firewall**.
  - On the Windows taskbar, click **Start** > **Programs** > **Norton Personal Firewall** > **Norton Personal Firewall**.
  - On the Windows XP taskbar, click **Start > More Programs > Norton Personal Firewall > Norton Personal Firewall**.
  - On the Windows desktop, double-click **Norton Personal Firewall**.

The Norton Personal Firewall main window appears.



Temporarily disabling Norton Personal Firewall

There may be times when you want to temporarily suspend a protection feature or the entire product. For example, you might want to see if Norton Personal Firewall is preventing a Web page from appearing correctly. Norton Personal Firewall lets you turn features off without adjusting the settings.

To temporarily disable Norton Personal Firewall

1. On the left side of the Norton Personal Firewall window, click **Internet Status > Current Status**.
2. In the Current Status window, click **Disable**.

You can also disable Norton Personal Firewall by right-clicking the Norton Personal Firewall icon in the notification area of the Windows taskbar and clicking Disable.

Norton Personal Firewall is enabled when you click Enable or the next time you start your computer.

Disabling a protection feature

You can disable a protection feature. For example, you might want to see if the Personal Firewall is preventing an application from operating correctly.

To disable a protection feature

1. On the left side of the Norton Personal Firewall window, click **Internet Status** > **Current Status**.
2. In the Current Status window, select the feature that you want to disable to open its status window.
3. In the feature's status window, click **Disable**.

The feature is enabled when you click Enable or the next time you start your computer.

Keeping current with LiveUpdate

Symantec products depend on current information to protect your computer from newly discovered threats. Symantec makes this information available to you through LiveUpdate. Using your Internet connection, LiveUpdate downloads program updates and protection updates to your computer.

Your normal Internet access fees apply when you use LiveUpdate.

About program updates

Program updates are minor improvements to your installed product. These differ from product upgrades, which are newer versions of entire products. Program updates that have self-installers to replace existing software code are also called patches. Patches are usually created to extend operating system or hardware compatibility, adjust a performance issue, or fix bugs.

LiveUpdate automates the process of downloading and installing program updates. It saves you the trouble of locating and downloading files from an Internet site, then installing them, and deleting the leftover files from your disk.

About protection updates

The intrusion protection service provides access to the latest predefined firewall rules and updated lists of applications that access the Internet. These lists are used to identify unauthorized access to your computer. Norton Personal Firewall uses the updates available from the intrusion protection service to detect the latest Internet threats.

About your subscription

Your Symantec product includes a complimentary, limited time subscription to protection updates for the subscription services used by your product. When that subscription is due to expire, you are prompted to renew your subscription. For more information, see "Subscription policy" on page 112.

If you do not renew your subscription, you can still use LiveUpdate to retrieve program updates. However, you cannot retrieve protection updates and will not be protected against newly discovered threats.

Obtain program and protection updates

Use LiveUpdate regularly to obtain program and protection updates.

Note: If you connect to the Internet through America Online (AOL), CompuServe, or Prodigy, connect to the Internet first, and then run LiveUpdate.

To obtain updates using LiveUpdate

1. Open your Symantec product.
2. At the top of the window, click **LiveUpdate**.

   You might receive a warning that your subscription has expired. Follow the on-screen instructions to complete the subscription renewal.
3. Click **Next** to locate updates.
4. If updates are available, click **Next** to download and install them.
5. When the installation is complete, click **Finish**.

Getting help with Norton Personal Firewall

There are four kinds of online Help:

- Comprehensive online Help
- Detailed instructions for windows and dialog boxes
- What's This? Help for buttons and other controls
- The Readme file and Release Notes

Comprehensive online Help

The online Help contains the information in this User's Guide.

To access Online Help

1. At the top of the Norton Personal Firewall window, click **Help**.
2. Click **Norton Personal Firewall Help**.

Window and dialog box Help

Dialog box Help provides information about the Norton Personal Firewall program. This type of Help is context-sensitive, meaning that it provides help for the dialog box or window that you are currently using.

To get help with a window or dialog box

- Do one of the following:
  - Click the **Tell Me More** link if one is available.
  - In the dialog box, click **Help**.

What's This? Help for buttons and other controls

What's This? Help provides a definition of individual components of a window or dialog box.

To access What's This? Help

- Right-click anywhere that you need help in a window or dialog box, then click **What's This?**

Readme file and Release Notes

The Readme file contains information about installation and compatibility issues. The Release Notes contain technical tips and information about product changes that occurred after this guide went to press. They are installed on your hard disk in the same location as the Norton Personal Firewall product files.

To read the Readme file

1. Do one of the following:
   - On the Windows taskbar, click **Start > Programs > Norton Personal Firewall > Product Support > readme.txt**.
   - On the Windows XP taskbar, click **Start > More Programs > Norton Personal Firewall > Product Support > readme.txt**.

   The file opens in Notepad.
2. Close the word processing program when you are done reading the file.

The Release Notes also can be accessed from the Start menu.

To read the Release Notes

1. Do one of the following:
   - On the Windows taskbar, click **Start > Programs > Norton Personal Firewall > Product Support > Norton Personal Firewall Release Notes**.
   - On the Windows XP taskbar, click **Start > More Programs > Norton Personal Firewall > Product Support > Norton Personal Firewall Release Notes**.

   The file opens in Notepad.
2. Close the word processing program when you are done reading the file.

Using the Security Assistant

The Security Assistant is always available to provide information on how Norton Personal Firewall works, or to change any of the settings you selected.

To use the Security Assistant

1. At the top of the Norton Personal Firewall window, click **Assistant**.
2. At the bottom of each pane, click **Next** to progress through the Security Assistant.
3. Click **Close** to close the Security Assistant.

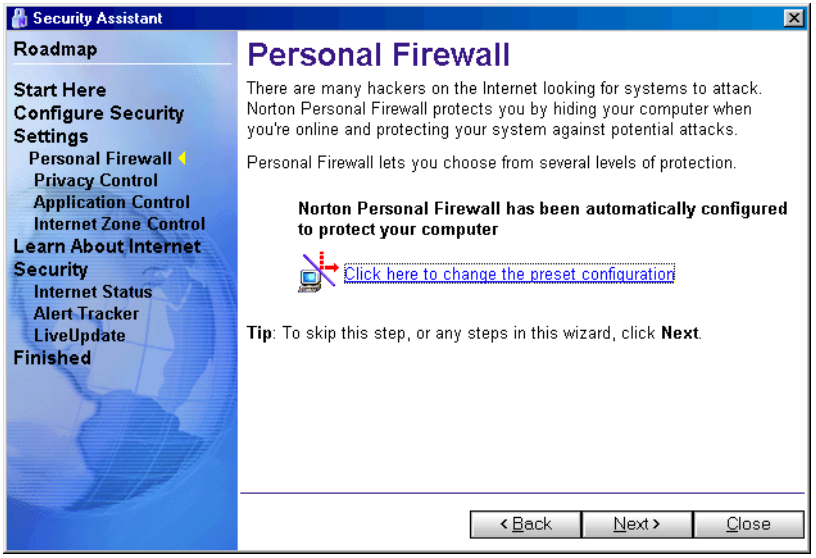
The purpose of each pane is described in the following sections.

Personal Firewall

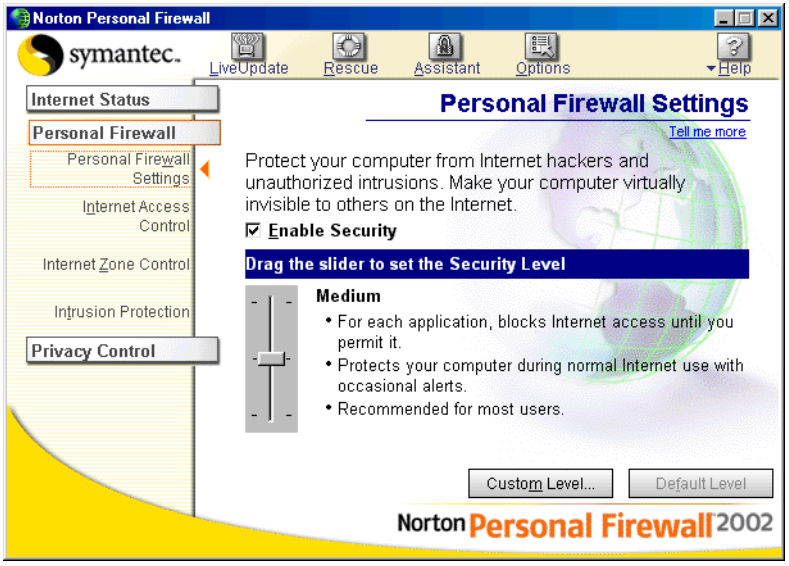
Personal Firewall protects your computer from unauthorized access while you are connected to the Internet. You can choose to have Personal Firewall enabled or disabled. If it is enabled (the default setting), you can also choose the level of protection provided.

To enable Personal Firewall

1. In the Security Assistant Roadmap, click **Personal Firewall**.


Security Assistant
Roadmap
Start Here
Configure Security Settings
Personal Firewall
Privacy Control
Application Control
Internet Zone Control
Learn About Internet Security
Internet Status
Alert Tracker
LiveUpdate
Finished
Personal Firewall
There are many hackers on the Internet looking for systems to attack. Norton Personal Firewall protects you by hiding your computer when you're online and protecting your system against potential attacks.
Personal Firewall lets you choose from several levels of protection.
Norton Personal Firewall has been automatically configured to protect your computer
Click here to change the preset configuration
Tip: To skip this step, or any steps in this wizard, click Next.
< Back
Next >
Close

2 Click **Click here to change the preset configuration**.



3 Check **Enable Security**.

For more information, see "Setting the Security Level" on page 62.

Privacy Control

Using Privacy Control, you can identify confidential information stored on your computer that should have extra protection. Any items that you put on this list are blocked from being released to any Web site that does not use secure, encrypted communications, and they are blocked from being sent through the supported instant messenger programs.

To add confidential information to be blocked

1 In the Security Assistant Roadmap, click **Privacy Control**.

2 In the Privacy Control pane, click **Add**.

3 In the Add Confidential Information dialog box, select a category in the Type of information to protect box.

4 In the Descriptive name field, type a description to help you remember why you are protecting the data.

5 In the Information to protect field, type the information you want to block from being sent through nonsecure Internet connections.

6 Click **OK**.

For more information, see "Adding confidential information to be blocked" on page 44.

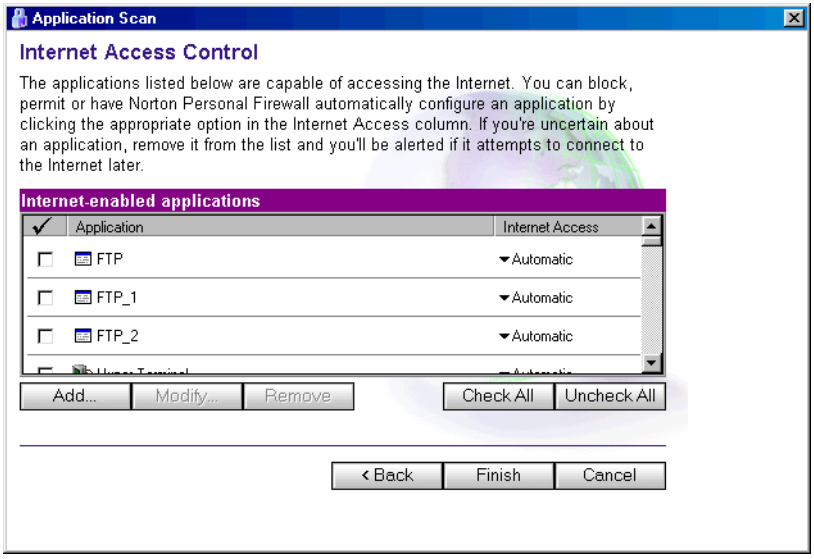
Application Control

Norton Personal Firewall can scan your computer for Internet-enabled applications and create access rules for them. When the scan is complete, you can use the results to determine which applications should have access to the Internet and, if desired, adjust their access rules.

To scan for Internet-enabled applications

1. In the Security Assistant Roadmap, click **Application Control**.
2. In the Application Control pane, click **Click here to scan for Internet applications**.
3. In the Application Scan window, click **Next** to begin the scan.

   When the scan is complete, all Internet-enabled applications that were found are listed.


Application Scan
Internet Access Control
The applications listed below are capable of accessing the Internet. You can block, permit or have Norton Personal Firewall automatically configure an application by clicking the appropriate option in the Internet Access column. If you're uncertain about an application, remove it from the list and you'll be alerted if it attempts to connect to the Internet later.
Internet-enabled applications
Application
Internet Access
FTP
Automatic
FTP_1
Automatic
FTP_2
Automatic
Add...
Modify...
Remove
Check All
Uncheck All
< Back
Finish
Cancel

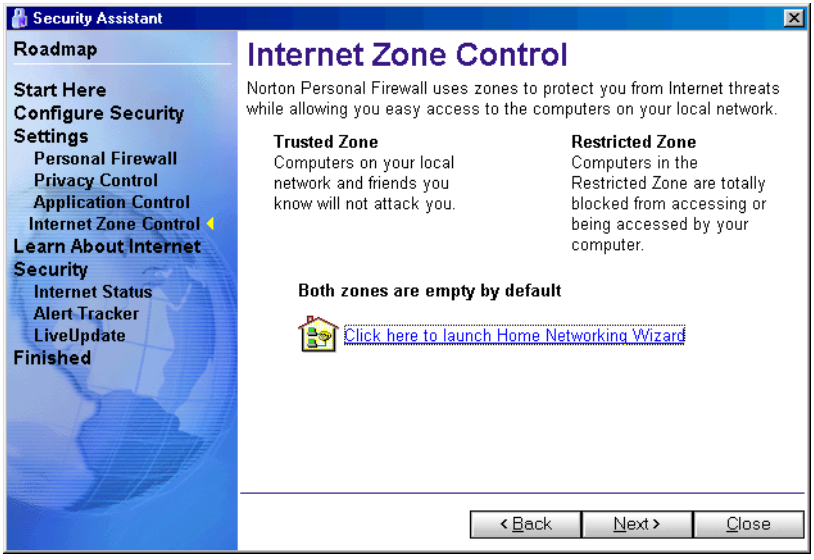
4. To allow Internet access for an application, check the box to the left of the application's name.
5. To change the Internet access rule or category of an application, select the setting you want from the appropriate drop-down list.
6. Click **Finish** when you are done.

Internet Zone Control

Use Internet Zone Control to identify computers to which you want to grant access to your computer and those to which you want to deny access. The Home Network Wizard can automatically configure your home network and add computers in that network to your Trusted Zone.

To run the Home Network Wizard from the Security Assistant

1 In the Security Assistant Roadmap, click **Internet Zone**.


Security Assistant
Roadmap
Start Here
Configure Security Settings
Personal Firewall
Privacy Control
Application Control
Internet Zone Control
Learn About Internet Security
Internet Status
Alert Tracker
LiveUpdate
Finished
Internet Zone Control
Norton Personal Firewall uses zones to protect you from Internet threats while allowing you easy access to the computers on your local network.
Trusted Zone
Computers on your local network and friends you know will not attack you.
Restricted Zone
Computers in the Restricted Zone are totally blocked from accessing or being accessed by your computer.
Both zones are empty by default
Click here to launch Home Networking Wizard
< Back
Next >
Close

2 In the Internet Zone Control pane, click **Click here to launch Home Networking Wizard**.

3 Follow the on-screen instructions.

For more information, see "Home network control with Internet Zone Control" on page 69.

Internet Status

Norton Personal Firewall tracks activity that occurs on your computer while you are connected to the Internet. You can check on this activity using Internet Status.

To check Internet Status

1. In the Security Assistant Roadmap, click **Internet Status**.
2. To see the current status of your Internet activity, click **Current Status**.

   For more information, see "Monitoring Norton Personal Firewall events" on page 77.
3. To adjust the amount of information displayed in Current Status, click **Reporting**.

   For more information, see "Adjusting the reporting detail" on page 58.

Alert Tracker

The Alert Tracker appears as a half globe on the side of your screen. When an event occurs on which Norton Personal Firewall reports, Alert Tracker briefly displays a message to inform you. For more information, see "Using Alert Tracker" on page 57.

LiveUpdate

LiveUpdate provides a way for you to receive program and protection updates. For more information, see "Keeping current with LiveUpdate" on page 31.

Running Security Check

Use Security Check to test your computer's vulnerability to security intrusions. The Security Check link in Norton Personal Firewall connects you to the Symantec Web site, on which you can get detailed information about what Security Check scans for, and from which you can run the scan.

To run Security Check

1. On the left side of the Norton Personal Firewall window, click **Internet Status > Security Check**.
2. In the Security Check window, click **Scan for Security Risks**.

   Your browser opens on the Symantec Security Check Web page.
3. To learn more about what Security Check does, in the Security Check Web page, click **About Scan for Security Risks**.
4. To run the scan, click **Scan for Security Risks**.

When the scan is complete, the results page lists all the areas checked and your level of vulnerability in each one. For any area marked as at risk, you can get more details about what the problem is and how to fix it.

To get more information about a scanned area

- In the results page, next to the scan name, click **Show Details**.

  If the area is at risk, the details include suggestions for fixing the problem.

CHAPTER 4

Protecting confidential information

Computers and Web sites collect personal information as you browse the Internet. A computer's security features might not always protect your personal information. Privacy Control helps protect your privacy by preventing these types of intrusions.

Privacy Control ensures that you don't send private information such as credit card numbers over the Internet unless they are encrypted, or you specifically allow it.

Web sites use *cookies* to track your Internet usage. While most sites use cookies to remember the choices you have made on that site, some sites use cookies to track your browsing habits. Norton Personal Firewall has several levels of control over cookies.

Your browser might provide more information than you like to the Web sites you visit. For example, most browsers give Web sites the address of the site you last visited. Privacy Control stops your browser from sending this type of information.

Setting the Privacy Level

The Privacy Level slider lets you select minimal, medium, or high privacy settings.

Setting	Description
High	All personal information is blocked from the Internet. An alert appears each time a cookie is encountered.
Medium (recommended)	An alert appears if confidential information is entered on a Web form or in an instant messenger. Conceals your browsing from Web sites. Cookies are not blocked.
Minimal	Confidential information is not blocked. Cookies are not blocked. Conceals your browsing from Web sites.

To set the Privacy Level

1. On the left side of the Norton Personal Firewall window, click **Privacy Control**.
2. Move the **Privacy Level** slider to the Privacy Level you want.

Adding confidential information to be blocked

There are many Web sites that ask for personal information that can jeopardize your privacy or let others steal from you. Also, any information sent using an instant messenger program is nonsecure.

For more information, see "Enabling secure Web connections" on page 47.

Norton Personal Firewall lets you create a list of personal information that is censored from all nonsecure Internet communications.

To add confidential information to be blocked

1. On the left side of the Norton Personal Firewall window, click **Privacy Control**.
2. Click **Confidential Info**.
3. In the Confidential Information dialog box, click **Add**.
4. In the Add Confidential Information dialog box, select a category in the Type Of Information To Protect box.
5. In the Descriptive Name field, type a description to help you remember why you are protecting the data.
6. In the Information To Protect field, type the information you want to block from being sent through nonsecure Internet connections.

Tips on entering confidential information

Because Norton Personal Firewall blocks personal information exactly the way that you enter it into the program, it is better to enter only partial numbers. For example, a phone number could be typed as 888-555-1234, but it could also be entered without dashes (8885551234) or with spaces (888 555 1234), or even in two or more separate boxes. One common aspect of these formats is that the last four digits (1234) are always together. Thus, you can have better protection by protecting the last four digits than you have by protecting the entire number.

Entering partial information has two advantages. First, you are not entering your complete credit card number where someone might find it. Second, it lets Norton Personal Firewall block your private information on sites that use multiple boxes for credit card numbers.

Adjusting privacy settings

You can change the settings for Confidential Information, Cookie Blocking, Browser privacy, and Secure Connections if the Privacy Level settings do not meet your needs.

Changing the Confidential Information setting

Confidential Information has three settings:

- High: Blocks all confidential information.
- Medium: Alerts you each time that you attempt to send confidential information to a nonsecure Web site or through an instant messenger.
- None: Does not block confidential information.

To change the Confidential Information setting

1. On the left side of the Norton Personal Firewall window, click **Privacy Control**.
2. Click **Custom Level**.
3. Select the Confidential Information setting that you want.

Changing the Cookie Blocking setting

Cookies are small files that your browser saves on your computer. Sometimes Web sites use them for information that makes it more convenient for you to use their sites.

Cookies that record personal information can jeopardize your privacy by letting others access them without your permission. They might contain enough information to show your browsing habits, or they could expose passwords and logon names.

When a Web site requests a cookie from your computer, Norton Personal Firewall checks to see whether you are permitting cookies, blocking cookies, or using Cookie Alerts to determine the action.

Cookie Blocking has three settings:

- High: Blocks all cookies.
- Medium: Alerts you each time a cookie is encountered.
- None: Allows cookies.

To change the Cookie Blocking setting

1. On the left side of the Norton Personal Firewall window, click **Privacy Control**.
2. Click **Custom Level**.
3. Select the Cookie Blocking setting that you want.

Enabling Browser Privacy

Browser Privacy prevents Web sites from retrieving the type of browser that you are using and finding out which Web site you last visited.

To enable Browser Privacy

1. On the left side of the Norton Personal Firewall window, click **Privacy Control**.
2. Click **Custom Level**.
3. In the Customize Privacy Settings dialog box, check **Enable Browser Privacy**.

Enabling secure Web connections

When you visit a secure Web site, your browser sets up an encrypted connection with the Web site. Information given over secure connections cannot be detected by a firewall because the information is encrypted. *Encryption* means that the information is encoded with a mathematical formula, scrambling the data into an unreadable format.

To enable secure Web connections

1. On the left side of the Norton Personal Firewall window, click **Privacy Control**.
2. Click **Custom Level**.
3. In the Customize Privacy Settings dialog box, check **Enable Secure Connections (https)**.

Blocking secure Web connections

To ensure that confidential information is not sent over secure Web connections, block all secure Web connections.

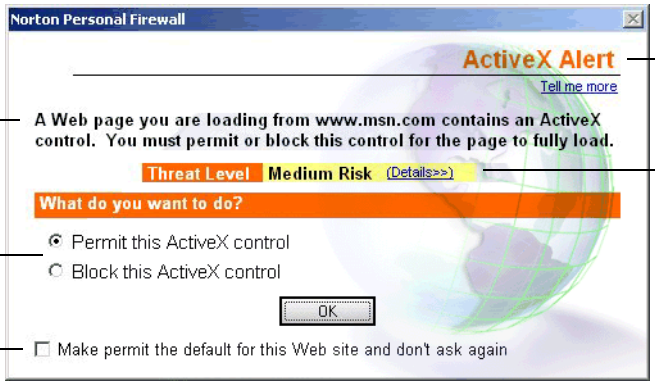
To block secure Web connections

1. On the left side of the Norton Personal Firewall window, click **Privacy Control**.
2. Click **Custom Level**.
3. In the Customize Privacy Settings dialog box, uncheck **Enable Secure Connections (https)**.

C H A P T E R 5

Responding to Norton Personal Firewall alerts

Norton Personal Firewall monitors communication activities to and from your computer and lets you know when an activity is taking place that may compromise your security.


Norton Personal Firewall
ActiveX Alert
Tell me more
A Web page you are loading from www.msn.com contains an ActiveX control. You must permit or block this control for the page to fully load.
Threat Level
Medium Risk
(Details>>)
What do you want to do?
Permit this ActiveX control
Block this ActiveX control
OK
Make permit the default for this Web site and don't ask again
Type of alert
Description of the problem that triggered the alert
Evaluation of the risk
Choices for responding to the alert
Make this choice permanent

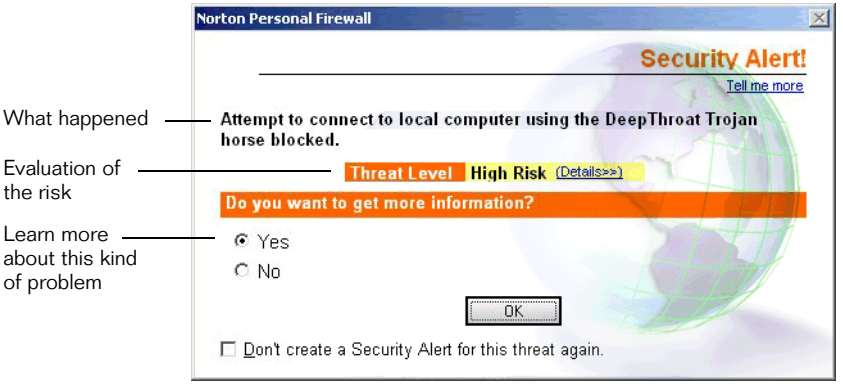
When an alert appears, read it before you make a decision. Identify what type of alert it is and the threat level. Once you understand the risks, you can make a choice.

Norton Personal Firewall shows the following types of alerts:

- Security Alerts
- Internet Access Control alerts
- ActiveX Alerts
- Java Alerts
- Cookie Alerts
- Confidential Information Alerts

Responding to Security Alerts

Security Alerts appear when someone attempts to access your computer. It may be a hacker or someone on your own network.


What happened
Evaluation of the risk
Learn more about this kind of problem
Norton Personal Firewall
Security Alert!
Tell me more
Attempt to connect to local computer using the DeepThroat Trojan horse blocked.
Threat Level High Risk (Details>>)
Do you want to get more information?
Yes
No
OK
Don't create a Security Alert for this threat again.

Most Security Alerts trigger AutoBlock, which prevents the computer that is attempting to connect to your computer from communicating with your computer for 30 minutes. This prevents attackers from repeatedly trying different attacks in an attempt to access your computer.

For more information, see "Using Intrusion Protection to stop attacks" on page 72.

Ensure that the alert describes a real attack and not a legitimate attempt to access your computer. If the attempt is legitimate, use Internet Access Control to allow the type of connection described in the alert.

For more information, see "Adding computers to zones" on page 70.

For more information, see "Adding an application to Internet Access Control" on page 68.

Don't assume that every Security Alert represents an attempt to hack into your computer. There are many more-or-less harmless events on the Internet that cause Security Alerts. Answer the following questions to determine if a Security Alert represents an actual attack or normal Internet activity:

- Is the connection attempt from an unknown computer?
- Does the Security Alert describe a clearly threatening behavior? Accessing a single closed port is not as threatening as a complete port scan.
- Is the attempt part of a pattern of threatening attempts from the same computer?

If you can't answer yes to all of these questions, you are probably not under attack. However, you might be seeing a hacker's scan of a number of computers looking for vulnerabilities. With Norton Personal Firewall enabled, your computer does not appear vulnerable to the hacker. In fact, your computer may not appear to exist to the hacker at all.

For more information, see "Understanding Internet risks" on page 101.

To respond to a Security Alert

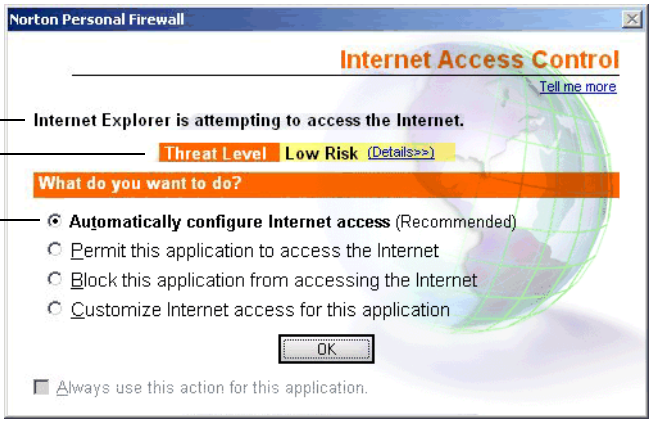
1. In the Security Alert window, click **Details** to read the information about this event.
2. Click **Yes** to learn more about this type of event.
3. If you decide that Norton Personal Firewall is blocking a legitimate activity, make the appropriate changes to your firewall protection or reporting.

   For more information, see "Customizing firewall protection" on page 61.

   For more information, see "Adjusting the reporting detail" on page 58.
4. Click **OK** to clear the event.

Responding to Internet Access Control alerts

Internet Access Control alerts appear when Norton Personal Firewall needs you to make a decision about an application on your computer that is attempting to access the Internet.


Norton Personal Firewall
Internet Access Control
Tell me more
What happened
Internet Explorer is attempting to access the Internet.
Evaluation of the risk
Threat Level
Low Risk
(Details>>)
What do you want to do?
Select Automatic if it is available: The application is recognized and appropriate rules are created
Automatically configure Internet access (Recommended)
Permit this application to access the Internet
Block this application from accessing the Internet
Customize Internet access for this application
OK
Always use this action for this application.

You can minimize the number of Internet Access Control alerts by doing an Application Scan, or by enabling Automatic Internet Access Control. When this option is enabled, Norton Personal Firewall creates rules for applications that it recognizes without interrupting your work.

For more information, see "Scanning for Internet-enabled applications" on page 67.

For more information, see "Enabling Automatic Internet Access Control" on page 67.

To respond to an Internet Access Control alert

1. In the Internet Access Control alert window, click **Details** to read the information about this event.
2. Do one of the following:
   - Click **Automatically configure Internet access** when it is available.

     Norton Personal Firewall recognizes the application and has appropriate access rules in its database. This is almost always the best option to select.
   - Click **Permit this application to access the Internet** to provide the application with full access to the Internet.

     This is not as safe as choosing Automatic, but it is appropriate for many applications that Norton Personal Firewall does not recognize. If you recognize the application and trust that it is safe, then this is the appropriate choice.
   - Click **Block this application from accessing the Internet** to block all Internet access for the application.

     This is the appropriate choice if you don't recognize the application and the risk is high.
   - Click **Customize Internet access for this application** to create specific rules for the application's Internet access.

     Select this option if you understand how the application accesses the Internet and you want to create specific rules to control its access. Choosing this option starts the Add Rule Wizard.

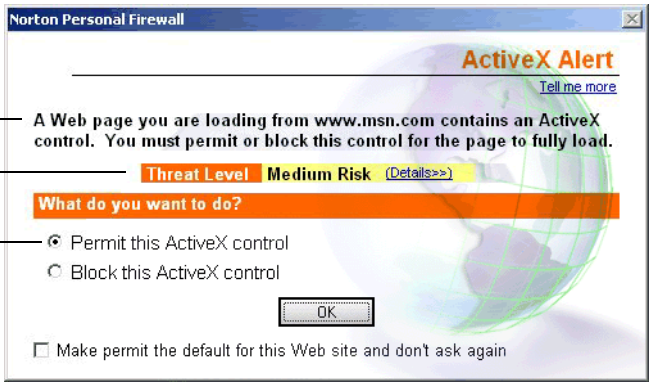
Responding to Java and ActiveX Alerts

Java applets and ActiveX controls are Web page components that do more than show text or graphics. Common applications of these components are pop-up menus and up-to-date stock quotes.

ActiveX and Java Alerts appear when you have the Security Level set to High, or have Java Applet Security or ActiveX Control Security set to Medium and a Java applet or ActiveX control is encountered.

For more information, see "Setting the Security Level" on page 62.

For more information, see "Setting Java and ActiveX Security Levels" on page 64.


Norton Personal Firewall
ActiveX Alert
Tell me more
A Web page you are loading from www.msn.com contains an ActiveX control. You must permit or block this control for the page to fully load.
Threat Level
Medium Risk
(Details>>)
What do you want to do?
Permit this ActiveX control
Block this ActiveX control
OK
Make permit the default for this Web site and don't ask again
What happened
Evaluation of the risk
Select Permit unless the Threat Level is high or you don't trust the source

To respond to a Java or ActiveX Alert

1. In the Java or ActiveX Alert window, Click **Details** to read the information about this event.
2. Do one of the following:
   - Click **Permit this ActiveX control (or Java applet)** to permit the ActiveX control or Java applet to run if you trust the integrity of the Web site.
   - Click **Block this ActiveX control (or Java applet)** to prevent the ActiveX control or Java applet from running.

     While this is always the safer option, it might prevent the Web page from appearing or functioning correctly. If you select block, and the Web page does not appear or function correctly, click your browser's Refresh button and choose Permit.

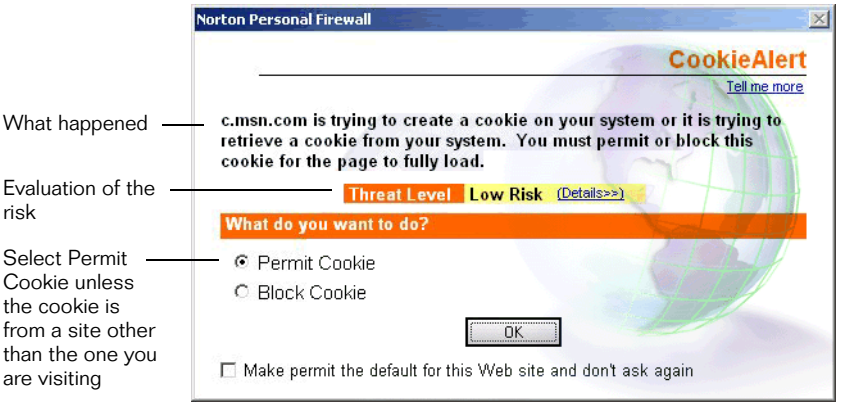
Responding to Cookie Alerts

Cookies are small files stored on your computer that Web sites use to track your visits.

Cookie Alerts appear when you have the Privacy Level set to High or Cookie Blocking set to Medium and you encounter a cookie.

For more information, see "Setting the Privacy Level" on page 44.

For more information, see "Changing the Cookie Blocking setting" on page 46.


What happened
Evaluation of the risk
Select Permit Cookie unless the cookie is from a site other than the one you are visiting
Norton Personal Firewall
CookieAlert
Tell me more
c.msn.com is trying to create a cookie on your system or it is trying to retrieve a cookie from your system. You must permit or block this cookie for the page to fully load.
Threat Level
Low Risk
(Details>>)
What do you want to do?
Permit Cookie
Block Cookie
OK
Make permit the default for this Web site and don't ask again

Because cookies are used so often and present a small security risk, you should not block cookies. However, cookies do present a significant risk to your privacy.

For more information, see "Understanding Internet risks" on page 101.

To block all cookies, and not see Cookie Alerts, change Cookie Blocking to High: Block Cookies.

To respond to a Cookie Alert

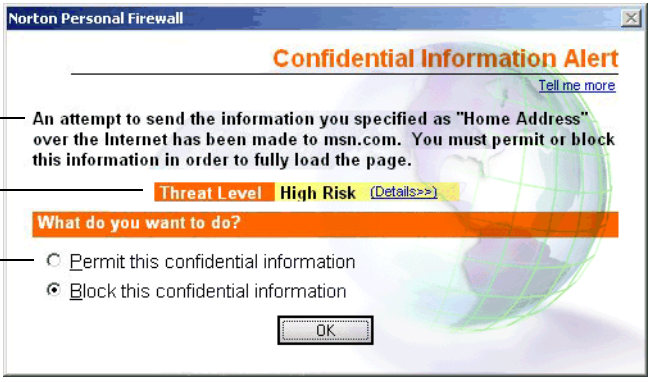
1. In the Cookie Alert window, click **Details** to read the information about this event.
2. Do one of the following:
   - Click **Permit this cookie** to allow the creation or access of the cookie.

     Cookies from the Web site that you are visiting are usually harmless and may be necessary for the Web pages to function.
   - Click **Block this cookie** to block the creation or access of the cookie.

     Expect repeated Cookie Alerts from pages on which you block cookies. Cookies that are from Web sites other than the one that you are visiting are commonly used to track your Internet usage, and can usually be blocked without affecting the operation of the Web site that you are visiting.

Responding to Confidential Information Alerts

Confidential Information Alerts appear when you attempt to send protected information to a Web site that does not use secure, encrypted communications, or when you send protected information using an instant messenger program.


Norton Personal Firewall
Confidential Information Alert
Tell me more
An attempt to send the information you specified as "Home Address" over the Internet has been made to msn.com. You must permit or block this information in order to fully load the page.
Threat Level
High Risk
(Details>>)
What do you want to do?
Permit this confidential information
Block this confidential information
OK
What happened
Evaluation of the risk
Select Permit this confidential information to allow this information to be sent

The alert includes the information that you attempted to send and to where it is being sent.

To respond to a Confidential Information Alert

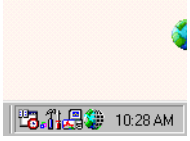
1. In the Confidential Information Alert window, click **Details** to read the information about this event.
2. Do one of the following:
   - Click **Permit this confidential information** to send the information.

     For example, select this option if you are trying to place an order.
   - Click **Block this confidential information** to stop the attempt to send the information.

There is a chance that Norton Personal Firewall recognizes other information as confidential information. For example, you might be entering a store's phone number in which the last four digits match the last four digits of your credit card number. In this case, permit the attempt to send the information.

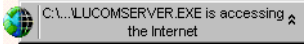
Using Alert Tracker

Alert Tracker keeps you up-to-date with the Norton Personal Firewall actions.



Alert Tracker rests on the side of your screen

When an event occurs that Norton Personal Firewall wants you to know about, but doesn't need to interrupt your work to tell you, Alert Tracker shows a message for a few seconds and then returns to the side of the screen.



Alert Tracker opens for a few seconds to show messages

Opening Alert Tracker

You can open Alert Tracker to see the most recent messages.

To Open Alert Tracker

- On the Windows desktop, double-click **Alert Tracker**.

Reviewing recent Alert Tracker messages

To review recent Alert Tracker messages

1. On the Windows desktop, double-click **Alert Tracker**.
2. To the right of the first message, click the up arrow if it appears.
3. Click on a message to see the Event Log.

Moving Alert Tracker

Alert Tracker attaches to either side of the screen on your primary monitor.

To move Alert Tracker

- Drag the half globe to the side of the screen where you want it to appear.

Hiding Alert Tracker

You can hide Alert Tracker if you don't want it to appear on your screen.

To hide Alert Tracker

- In the notification area of the Windows taskbar, right-click the Norton Personal Firewall icon, then click **Hide Alert Tracker**.

Adjusting the reporting detail

The Reporting Level controls the amount of information that appears in Alert Tracker and the number of Security Alerts that appear.

Setting the Reporting Level

The Reporting Level slider lets you select Minimal, Medium, or High Reporting levels. When you change the slider position, the reporting level changes.

Setting	Description
High	Provides the most complete information about Norton Personal Firewall activities. Shows the most Alert Tracker messages. Notifies you of applications accessing the Internet and Security Alerts.
Medium (recommended)	Provides information about important Internet events. Shows a medium number of Alert Tracker messages. Notifies you of Security Alerts and Automatic Internet Access Control alerts.
Minimal	Provides information about critical Internet events. Notifies you of Security Alerts and Automatic Internet Access Control alerts.

To set the Reporting Level

1. On the left side of the Norton Personal Firewall window, click **Internet Status > Reporting**.
2. Move the slider to the Reporting Level that you want.

CHAPTER 6

Customizing firewall protection

Norton Personal Firewall protects your computer from unauthorized access attempts. It blocks attacks from other computers and controls Internet access for applications on your computer.

The firewall provides four types of protection:

- Norton Personal Firewall provides an overall Security Level setting that makes appropriate adjustments throughout the program.
- Internet Access Control sets access rules for the applications on your computer.
- Internet Zone Control lets you access trusted computers and completely block restricted computers.
- Intrusion Protection monitors hacker attacks on your computer and blocks computers that attack you from further access.

Setting the Security Level

The Security Level makes settings throughout Norton Personal Firewall that are appropriate to the Security Level that you select. It changes the firewall setting, and the settings for Java applets and ActiveX controls. It controls whether unused ports respond to access attempts.

The slider lets you select Minimal, Medium, or High security settings. When you change the slider position, the protection level changes.

Setting	Description
High	Firewall is set to High, which blocks everything until you allow it. If you have done an Application Scan, you should not be interrupted frequently with Internet Access Control alerts. ActiveX Control and Java Applet Security is set to Medium, which prompts you each time one is encountered. Unused ports do not respond to connection attempts, giving them a stealth appearance.
Medium (recommended)	Firewall is set to High, which blocks everything until you allow it. If you have done an Application Scan, you should not be interrupted frequently with Internet Access Control alerts. ActiveX Control and Java Applet Security is set to None, which lets all ActiveX controls and Java applets run. Unused ports do not respond to connection attempts, giving them a stealth appearance.
Minimal	Firewall is set to Medium, which blocks connection attempts to Trojan horse programs. ActiveX Control and Java Applet Security is set to None, which lets all ActiveX Controls and Java applets run.

For more information, see "Scanning for Internet-enabled applications" on page 67.

To set the Security Level

1. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Personal Firewall Settings**.
2. Move the slider to the Security Level that you want.

Making custom security settings

If the Security Level options do not meet your needs, you can change the settings for the Firewall, Java, and ActiveX protection levels.

Changing the Personal Firewall setting

The firewall monitors communications between your computer and other computers on the Internet. It monitors both connection attempts from other computers and attempts by applications on your computer to connect to other computers.

Norton Personal Firewall has three settings:

Setting	Description
High	Blocks all communication that you do not specifically allow. You must create firewall rules for every application that requests Internet access. If you have done an Application Scan, you should not be interrupted frequently with Internet Access Control alerts.
Medium	Blocks many ports used by harmful applications. However, it can also block useful applications when they use the same ports.
None	Disables the firewall and allows all Internet communications.

For more information, see "Scanning for Internet-enabled applications" on page 67.

To change the Personal Firewall setting

1. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Personal Firewall Settings**.
2. Click **Custom Level**.
3. Select the Personal Firewall setting that you want.

Setting Java and ActiveX Security Levels

Java applets and ActiveX controls make Web sites more interactive. Many Web sites rely on ActiveX controls and Java applets to perform and appear correctly. Most of these applications are safe and do not threaten your system or data.

However, ActiveX controls can have total access to your data, depending on how they are programmed. They can copy data from your hard disk and transmit it over the Internet while you are online. They can delete files, intercept messages, capture passwords, or gather banking numbers and other important data.

The only way to prevent bad applications from running on your computer is to block them from downloading. However, blocking all Java applets and ActiveX controls prevents many Web sites from appearing or running correctly.

In the Customize Security Settings dialog box, the Java Applet Security and ActiveX Control Security features have three options:

Setting	Description
High	Blocks your browser from running any Java applets or ActiveX controls over the Internet. This is the safest, but most inconvenient option. Web sites that rely on these elements might not operate properly using this setting.
Medium	Prompts you when Java applets and ActiveX controls are encountered. This lets you temporarily or permanently allow or block each Java applet or ActiveX control that you encounter. It can be bothersome to respond every time you come across a Java applet or ActiveX control, but it lets you decide which ones to run.
None	Lets Java applets and ActiveX controls run whenever you encounter them.

To set Java and ActiveX security levels

1. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Personal Firewall Settings**.
2. Click **Custom Level**.
3. Select the Java Applet Security setting or ActiveX Control Security setting that you want.

Enabling Internet Access Control alerts

Internet Access Control alerts give you control when an application tries to connect to the Internet but no firewall rule exists for it. When a connection attempt is made, an Internet Access Control alert appears, and you can permit or block the application from accessing the Internet.

Disable this option to block applications from accessing the Internet when there are no specific firewall rules in place for them.

To enable Internet Access Control alerts

1. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Personal Firewall Settings**.
2. Click **Custom Level**.
3. Check **Enable Access Control Alerts**.

Enabling alerts for unused ports

Norton Personal Firewall blocks access to the unused ports on your computer.

For example, if someone tries to connect to your computer using Symantec pcAnywhere and you don't have a pcAnywhere host running, no response is made to acknowledge the connection attempt so the inquiring computer learns nothing.

You can see alerts when an attempt is made to access an unused port on your computer. These alerts are useful for solving problems when you are configuring advanced programs and features such as Internet Connection Sharing. Disable to avoid alerts about harmless connection attempts.

To enable alerts for unused ports

1. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Personal Firewall Settings**.
2. Click **Custom Level**.
3. Check **Alert when unused ports are accessed**.

Controlling applications that access the Internet

Applications access the Internet for many reasons. Your Web browser accesses the Internet so that you can view Web pages. LiveUpdate accesses the Internet to retrieve program and protection updates for your Symantec products. Microsoft NetMeeting accesses the Internet to let you conduct meetings over the Internet.

Each of these applications has different requirements for accessing the Internet. Some, such as LiveUpdate, have simple requirements. Others, such as Internet Explorer, have complex requirements.

Internet Access Control maintains a list of the applications on your computer that access the Internet. The list records the applications' requirements, and whether Internet access is allowed or blocked.

There are several ways to add applications to the Internet Access Control list:

- Scan for Internet-enabled applications: Finds and configures access for all of your Internet-enabled applications at once.

  For more information, see "Scanning for Internet-enabled applications" on page 67.

- Enable Automatic Internet Access Control: Automatically configures access for well-known applications the first time that you run them.

  For more information, see "Enabling Automatic Internet Access Control" on page 67.

- Respond to alerts: Norton Personal Firewall alerts you the first time each Internet-enabled application attempts to access the Internet. You can then allow or block access. If the application is recognized by Norton Personal Firewall, it suggests that you use the automatic configuration option.

  For more information, see "Responding to Internet Access Control alerts" on page 52.

- Add applications individually: You can add applications to the list on the Internet Access Control screen.

  For more information, see "Adding an application to Internet Access Control" on page 68.

Scanning for Internet-enabled applications

Scanning for Internet-enabled applications is the quickest way to set up Internet Access Control for all of your applications. Norton Personal Firewall scans your computer for applications that it recognizes and then lets you choose appropriate settings for each application.

To scan for Internet-enabled applications

1. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Internet Access Control**.
2. Click **Configure**, then click **Application Scan**.
3. Follow the on-screen instructions.

Enabling Automatic Internet Access Control

When Automatic Internet Access Control is enabled, Norton Personal Firewall automatically creates a new firewall rule for applications that it has digital signatures (fingerprints) for the first time the applications are run.

Disable this option if you want to be notified when a new application attempts to access the Internet.

Be sure to run LiveUpdate weekly to retrieve program and protection updates.

To enable Automatic Internet Access Control

1. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Internet Access Control**.
2. Click **Configure**, then check **Enable Automatic Internet Access Control**.

Responding to Internet Access Control alerts

If Automatic Internet Access Control is not enabled, or Norton Personal Firewall encounters an application that it does not recognize attempting to access the Internet, an Internet Access Control alert appears.

If the option Automatically configure Internet access appears in the alert, then Norton Personal Firewall knows about the application and can configure appropriate access.

If Automatically configure Internet access does not appear, the application is not recognized by Norton Personal Firewall and you must decide whether or not to allow access to the application. Review the threat level before you make your decision.

If Automatically configure Internet access appears in the alert but is disabled, then Norton Personal Firewall knows about the application but does not expect the communication attempt as part of the application's normal operation.

For more information, see "Responding to Internet Access Control alerts" on page 52.

Adding an application to Internet Access Control

You can manually add applications to the list of applications in Internet Access Control. Use this method if you have an application with specific Internet access requirements and you understand firewall rules.

To add an application to Internet Access Control

1. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Internet Access Control**.
2. Click **Add**.
3. Select the application's executable file.
4. Click **Open**.
5. In the Internet Access Control window, follow the on-screen instructions.

Changing Internet Access Control settings

You can change the Internet Access Control settings for applications. For example, you may decide that you want to allow access to an application that is blocked.

To change Internet Access Control settings

1. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Internet Access Control**.
2. Under Internet Access, select the entry for the application that you want to change.
3. On the drop-down menu, select a new setting.

Changing system-wide settings

System-wide settings provide protection that is broader than those covering a single application. For example, protection against someone attaching to your computer using Microsoft networking is provided in system-wide settings.

System-wide settings provide a series of rules that the firewall uses to allow or block various activities. While you can add to or change these rules, you should have a good understanding of what they do to ensure that you don't compromise your protection.

To change system-wide settings

1. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Internet Access Control**.
2. Click **Configure**, then click **System-Wide Settings**.

Home network control with Internet Zone Control

Internet Zone Control provides an easy way for you to identify computers that you trust not to attack you, and computers that you specifically want to restrict from accessing your computer. There are two zones: Trusted and Restricted.

Computers that you place in the Trusted zone are not regulated by Norton Personal Firewall. They have as much access to your computer as they would have if Norton Personal Firewall was not installed. Use the Trusted zone for computers on your local network with which you need to share files and printers.

If a computer in your Trusted zone is attacked, and a hacker takes control of it, it poses a risk to your computer.

Computers that you place in the Restricted zone are prevented from accessing your computer at all. Add computers that repeatedly attempt to attack you to the Restricted zone. The Restricted zone provides the highest level of protection, beyond the normal protection provided by Norton Personal Firewall. You cannot interact with computers in the Restricted zone at all.

Adding computers to zones

Add computers that you trust to the Trusted zone. Add computers that you want to totally block to the Restricted zone.

To add computers to a zone

1. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Internet Zone Control**.
2. Select the zone to which you want to add a computer.
3. Click **Add**.

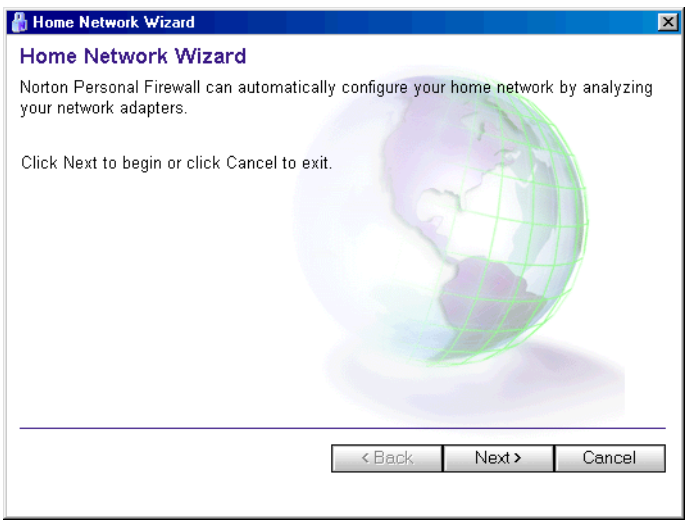
   You can add a single computer or a group of computers. For more information, see "Identifying computers to Norton Personal Firewall" on page 74.

Adding computers on your home network to the Trusted zone

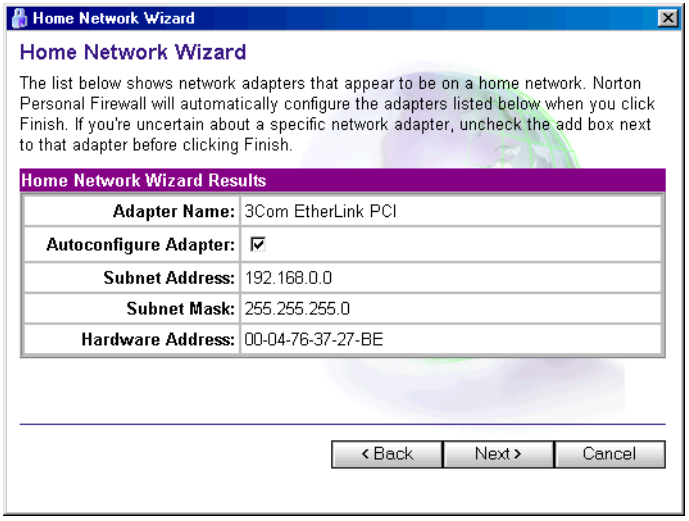
The Home Network Wizard provides the easiest way for you to identify other computers on your home network with which you want to share files or printers.

To add the computers on your home network to the Trusted zone

1. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Internet Zone Control**.
2. In the Internet Zone Control pane, click **Wizard**.

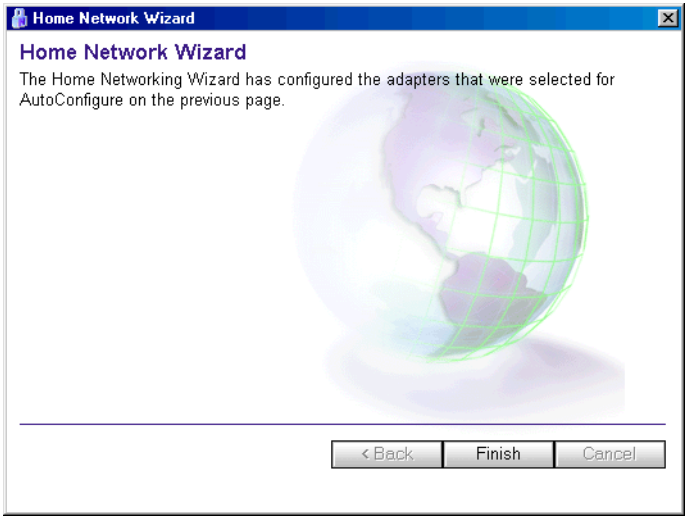

Home Network Wizard
Home Network Wizard
Norton Personal Firewall can automatically configure your home network by analyzing your network adapters.
Click Next to begin or click Cancel to exit.
< Back
Next >
Cancel

3 Click **Next** to begin the Wizard.


Home Network Wizard
Home Network Wizard
The list below shows network adapters that appear to be on a home network. Norton Personal Firewall will automatically configure the adapters listed below when you click Finish. If you're uncertain about a specific network adapter, uncheck the add box next to that adapter before clicking Finish.
Home Network Wizard Results
Adapter Name: 3Com EtherLink PCI
Autoconfigure Adapter:
Subnet Address: 192.168.0.0
Subnet Mask: 255.255.255.0
Hardware Address: 00-04-76-37-27-BE
< Back
Next >
Cancel

4 In the resulting list, check the network adapters that you want configured automatically and added to your Trusted zone.

5 Click **Next**.


Home Network Wizard
Home Network Wizard
The Home Networking Wizard has configured the adapters that were selected for AutoConfigure on the previous page.
< Back
Finish
Cancel

6 Click **Finish** to close the Home Network Wizard.

Using Intrusion Protection to stop attacks

Intrusion Protection stops hacker attacks as they occur. Norton Personal Firewall monitors Internet communications, looking for patterns of communications that are typical of a hacker attack. For example, if a computer tries to connect to a series of ports on your computer, Intrusion Protection recognizes it as a port scan, which is a common method of finding weaknesses to attack.

Intrusion Protection also detects attempts to connect to ports used by remote-access Trojan horse programs.

For more information, see "Understanding Internet risks" on page 101.

You can review and control the reaction to attacks in the Intrusion Protection window.

Detecting Port Scan Attempts

To be notified when Norton Personal Firewall detects a port scan or other attack, enable Detect Port Scan Attempts.

To enable Detect Port Scan Attempts

1. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Intrusion Protection**.
2. Check **Detect Port Scan Attempts**.

Enabling AutoBlock

When Norton Personal Firewall detects an attack, it warns you and blocks all communications from the attacking computer for 30 minutes. This automatic blocking of communications is called AutoBlock.

AutoBlock stops all communication from the remote computer for 30 minutes. It does not stop you from communicating to the remote computer.

Computers in the Trusted and Restricted zones are not subject to AutoBlock. Computers in the Trusted zone are never blocked, while computers in the Restricted zone are permanently blocked.

To enable AutoBlock

1. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Intrusion Protection**.
2. Check **Enable AutoBlock**.

Unblocking a blocked computer

In some cases, Norton Personal Firewall may recognize normal activity as an attack. If you can't communicate with a computer with which you should be able to communicate, see if it is on the list of Computers currently blocked by AutoBlock.

If a computer that you need to access appears on the list of Computers currently blocked by AutoBlock, unblock it.

To unblock a single blocked computer

1. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Intrusion Protection**.
2. Select the IP address of the computer that you want to unblock.
3. Click **Unblock**.

Excluding specific activities from AutoBlock

Some normal Internet activities will be repeatedly recognized by Norton Personal Firewall as an attack. For example, some Internet service providers scan the ports of client computers to ensure that they are within their service agreements.

To prevent normal activities from interrupting your Internet use, you can exclude these activities from being blocked by AutoBlock.

To exclude activities from AutoBlock

1. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Intrusion Protection**.
2. Click **Exclusions**.
3. In the Currently blocked list, select the IP address that you want to exclude.
4. Click **Exclude**.

Restricting a blocked computer

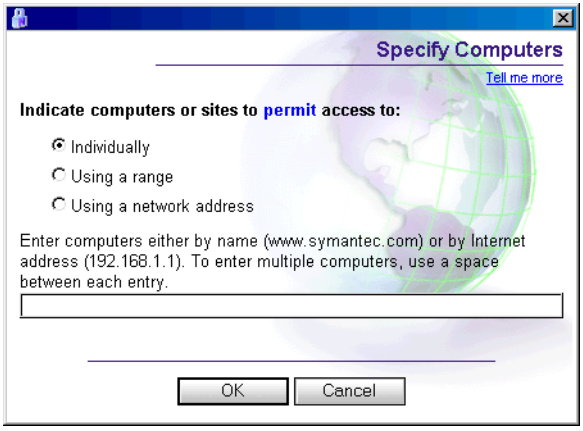
You can add a blocked computer to your Restricted zone to permanently prevent that computer from accessing your computer. Computers added to the Restricted zone do not appear on the blocked list.

To restrict a blocked computer

1. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Intrusion Protection**.
2. In the list of computers currently blocked by AutoBlock, select the computer to add to the Restricted zone, then click **Restrict**.

Identifying computers to Norton Personal Firewall

There are several places in Norton Personal Firewall in which you might need to identify computers to the program. In each case, the Specify Computers dialog box appears.


Specify Computers
Tell me more
Indicate computers or sites to permit access to:
Individually
Using a range
Using a network address
Enter computers either by name (www.symantec.com) or by Internet address (192.168.1.1). To enter multiple computers, use a space between each entry.
OK
Cancel

The Specify Computers dialog box lets you specify computers in three ways. In each you can use IP addresses to identify computers.

For more information, see "About the Internet" on page 93.

Specifying individual computers

IP addresses are 32-bit numbers expressed as four decimal numbers, each ranging from 0 to 255, and separated by periods. For example: 206.204.52.71.

The computer name that you type can be a URL (Uniform Resource Locator), such as service.symantec.com, or a Microsoft Network computer name, such as Mojave. You can find the names of computers on your local network in Network Neighborhood or Network Places.

Note: If you don't have TCP/IP bound to Client for Microsoft Networks in Windows Network Properties, you must use IP addresses instead of names for the computers on your local network.

To specify an individual computer

1. In the Specify Computers window, click **Individually**.
2. Type the name or IP address of a single computer.

Specifying a range of computers

You can enter a range of computers by specifying the starting (lowest numerically) IP address and the ending (highest numerically) IP address. All of the computers within that range of IP addresses are included.

In almost every case, the first three of the four numbers of the IP addresses entered should be the same.

To specify a range of computers

1. In the Specify Computers window, click **Using a range**.
2. In the Starting Internet Address field, type the starting (lowest numerically) IP address.
3. In the Ending Internet Address field, type the ending (highest numerically) IP address.

Specifying computers using a network address

You can identify all the computers on a single subnet by specifying an IP address and a subnet mask.

The IP address you specify can be any address in the subnet that you are identifying. The appropriate subnet mask is almost always 255.255.255.0.

For more information, see "How computers are identified on the Internet" on page 100.

To specify computers using a network address

1. In the Specify Computers window, click **Using a network address**.
2. In the Network Address field, type the IP address of a computer on the subnet.
3. In the Subnet Mask field, type the subnet mask.

CHAPTER 7

Monitoring Norton Personal Firewall events

Norton Personal Firewall provides information about its activities.

- The Current Status window shows several sets of counters indicating current Web- and firewall-related activities.
- The Event Log records actions that Norton Personal Firewall has taken and records your Internet activities.
- The Statistics window displays statistics of network activity and actions that Norton Personal Firewall has taken.

Reviewing Current Status

Current Status gives you a view of the current state of Norton Personal Firewall. It displays status for the following:

- Personal Firewall
- Privacy

Checking Personal Firewall status

Personal Firewall status provides information about recent attacks on your computer, including the time of the most recent attack and the IP address of the computer that attacked you.

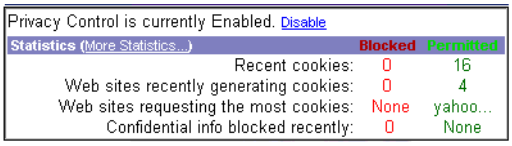
Personal Firewall is currently Enabled. Disable
Statistics (More Statistics...)
You were last attacked on: Fri Feb 9 13:40:15 PST 2001
Recent intrusion attempts: 3
Recent attempted attackers: 1
Most frequent attacker: 10.0.0.242

To check Personal Firewall status

1. On the left side of the Norton Personal Firewall window, click **Internet Status** > **Current Status**.
2. Click **Personal Firewall**.

Checking Privacy status

Privacy Control status shows you how many cookies have been blocked or permitted, and how many times you have sent or blocked confidential information.


Privacy Control is currently Enabled. Disable
Statistics (More Statistics...) Blocked Permitted
Recent cookies: 0 16
Web sites recently generating cookies: 0 4
Web sites requesting the most cookies: None yahoo...
Confidential info blocked recently: 0 None

To check privacy status

1. On the left side of the Norton Personal Firewall window, click **Internet Status** > **Current Status**.
2. Click **Privacy Control**.

CHAPTER 8

Configuring Norton Personal Firewall for common situations

Norton Personal Firewall can be configured to meet your needs in many different situations. This section describes the appropriate settings for a number of common situations.

Using Norton Personal Firewall with a dial-up connection

As installed, Norton Personal Firewall is properly configured to provide protection with a dial-up connection.

Using Norton Personal Firewall with a broadband connection

As installed, Norton Personal Firewall is properly configured to provide protection with a broadband connection, such as a cable modem or DSL service.

The most important thing in maintaining your protection from Internet risks is to keep Norton Personal Firewall enabled. Because most broadband connections are always active, your computer can be attacked at any time.

Troubleshooting broadband problems

Common broadband problems include:

- NetBIOS name is required.
- ISP periodically scans your computer.

NetBIOS name is required

A few cable systems require that your computer make its NetBIOS name visible. The NetBIOS name is visible, while the files and folders on your computer remain hidden.

To make your NetBIOS name visible

1. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Internet Access Control**.
2. Click **Configure** and select **System-Wide Settings**.
3. In the System-Wide Settings dialog box, select Default Inbound NetBIOS Name, then click **Modify**.
4. On the Action tab of the Modify Rule dialog box, click **Permit Internet access**.
5. Click **OK**.
6. In the System-Wide Settings dialog box, click **OK**.

ISP periodically scans your computer

Some broadband systems scan the ports on users' computers to ensure that they are keeping to their service agreements. Norton Personal Firewall might interpret this as a malicious port scan and stop communications with your ISP.

If this occurs, follow these steps to allow ISP port scans.

To allow ISP port scans

1. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Intrusion Protection**.
2. In the Intrusion Protection window, click **Exclusions**.
3. In the Exclusions dialog box, select the ISP that is currently blocked, then click **Exclude**.
4. Click **OK**.

Using Norton Personal Firewall with multiplayer games

Some multiplayer games require special Internet access. If you have trouble with your games, give the game application full permission to access the Internet. If that doesn't work, temporarily put the computers of the other players in the Trusted zone.

Giving a multiplayer game access to the Internet

The first step to making a multiplayer game work is to give it permission to access the Internet.

To give a multiplayer game access to the Internet

1. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Internet Access Control**.
2. Click **Add**.
3. Select the application's executable file, then click **Open**.
4. In the Internet Access Control window, click **Permit <application> access to the Internet**.
5. Click **OK**.

Note: If the application is already listed, click its entry under Internet Access and choose Permit All.

Placing other players in the Trusted zone

If giving the game application access to the Internet doesn't work, temporarily place the computers of the other players in your Trusted zone.

To place other players in the Trusted zone

1. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Internet Zone Control**.
2. On the Trusted tab, click **Add**.
3. Enter the IP addresses of the other players.

Using Norton Personal Firewall on a home network

Norton Personal Firewall protects you from Internet risks while allowing you full use of your local network.

For your safety, Norton Personal Firewall prevents local network activity when it is installed. This prevents someone from connecting to your computer over the Internet using Microsoft Networking.

Enabling file and printer sharing

Microsoft networking provides file and printer sharing. You can enable these features on your local network, while protecting them from the Internet.

To enable file and printer sharing

1. Open Windows Explorer.
2. Expand **Network Neighborhood** or **My Network Places** to locate the names of the computers on your local network.
3. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Internet Zone Control**.
4. On the Trusted tab, click **Add**.
5. Add each of the local computers to the Trusted zone.

For more information, see "Adding computers to zones" on page 70.

You can also unblock file and printer sharing using the System-Wide Settings.

To unblock file and printer sharing

1. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Internet Access Control**.
2. Click **Configure** and select **System-Wide Settings**.
3. In the System-Wide Settings dialog box, select the entry for Windows file sharing or printer sharing, then click **Modify**.
4. On the Action tab of the Modify Rule dialog box, click **Permit Internet access**.
5. Click **OK**.
6. In the System-Wide Settings dialog box, click **OK**.

Internet connection sharing

Norton Personal Firewall works with Internet connection sharing.

For full protection, install Norton Personal Firewall on each computer on your home network. Installing Norton Personal Firewall on the gateway computer protects your network from many outside attacks, but cannot protect against Trojan horses or other problem applications that initiate outbound connections unless it is installed on each computer on the network.

Using Norton Personal Firewall with a cable or DSL router

Norton Personal Firewall works behind a cable or DSL router and adds to the protection provided by the router. In some cases, you might want to reduce the protection provided by the router so that you can use applications like NetMeeting or Microsoft Messenger.

Norton Personal Firewall also provides features that might not be available with cable and DSL routers, such as privacy protection.

Using Norton Personal Firewall on a corporate network

If you use your computer at home and at work, you might need to use Norton Personal Firewall behind a corporate firewall.

Enabling file and printer sharing

If you don't want to disable Norton Personal Firewall, you can enable file and printer sharing so your computer works on an office network.

To enable file and printer sharing

1. Open Windows Explorer.
2. Expand **Network Neighborhood** or **My Network Places** to locate the names of the computers on your local network.
3. On the left side of the Norton Personal Firewall window, click **Personal Firewall** > **Internet Zone Control**.
4. On the Trusted tab, click **Add**.
5. Add each of the local computers to the Trusted zone.

For more information, see "Adding computers to zones" on page 70.

You can also unblock file and printer sharing. For more information, see "To unblock file and printer sharing" on page 83.

Administrative software on corporate networks

Administrative software used on some corporate networks may cause alerts from Norton Personal Firewall. If you experience unusual alerts while working on a corporate network, disable Norton Personal Firewall or talk to your network administrator.

Using Norton Personal Firewall with a proxy server

Norton Personal Firewall works with most proxy servers. However, you might have to change some settings to maintain full protection.

Determining whether Norton Personal Firewall works with your proxy server

The first step in making this determination is to find out if Norton Personal Firewall works with your proxy server.

To determine whether Norton Personal Firewall works with your proxy server

1. At the top of the Norton Personal Firewall window, click **Options**.
2. Click **View Statistics**.
3. In the Web category, look at the Bytes Processed counter.
4. Use your browser to connect to a Web site.

   If Norton Personal Firewall is filtering, the Bytes Processed counter in the Statistics window should increase as you access Web pages. If the Bytes Processed counter stays at 0, then Norton Personal Firewall is probably not monitoring the port used by your proxy server.

Determining which port to monitor for HTTP communication

If Norton Personal Firewall does not work with your proxy server, check the port that your proxy server is using for HTTP communications.

To determine which port to monitor for HTTP communication

1. Use your browser to connect to a Web site.
2. At the top of the Norton Personal Firewall window, click **Options**.
3. Click **View Event Log**.
4. On the Connections tab, look at the information in the Remote column.

   There should be a port number following the IP address of the site that you viewed with your browser. This number is the port number that was used to access your proxy server for your Web connection.
5. Record the port number.

Specifying which ports to monitor for HTTP communication

Your computer may connect to the Internet through a proxy server, which causes all HTTP communication to go through the port used by the proxy server.

To specify which ports to monitor for HTTP communication

1. At the top of the Norton Personal Firewall window, click **Options**.
2. Click **Advanced Options**.
3. On the Other tab, do one of the following:
   - Click **Add**, then enter the number of the port that you want to monitor for HTTP communication to add a port to the HTTP Port List.
   - Select the port number in the HTTP Port List, then click **Remove** to remove a port from the HTTP Port List.

Running a Web server with Norton Personal Firewall

When properly configured, Norton Personal Firewall will not prevent you from running a Web server.

To allow a Web server to run behind Norton Personal Firewall, you must create a rule that allows inbound TCP connections on port 80.

To configure Norton Personal Firewall for a Web server

1. View your Web site by entering the IP address in the address bar of your browser.

   Norton Personal Firewall displays an Internet Access Control alert.
2. In the alert dialog box, click **Automatically configure Internet access**.

Running an FTP server with Norton Personal Firewall

To allow an FTP server to run behind Norton Personal Firewall, you must create the following:

- A rule that allows inbound TCP connections on port 21
- A rule that allows outbound TCP connections on port 22
- A rule that allows inbound TCP connections on ports 1024 to 5000

To configure Norton Personal Firewall for an FTP server

1. View your FTP site by typing **FTP://** followed by the IP address of your FTP server in the address bar of your browser.

   Norton Personal Firewall displays an Internet Access Control alert.

2. In the alert dialog box, click **Customize Internet access for this application**.

   For more information, see "Responding to Internet Access Control alerts" on page 52.

Using Norton Personal Firewall with DHCP

If your computer gets its IP address from a DHCP server that provides a different IP address each time, you need to be careful when you enter local addresses in rules.

Instead of entering a single IP address, which might change at any time, enter a network address using a base IP address and a subnet mask. Enter values that cover the range of addresses that might be assigned to your computer.

For more information, see "Identifying computers to Norton Personal Firewall" on page 74.

Using Norton Personal Firewall with pcAnywhere

You should have no problems using pcAnywhere as either a client or host with Norton Personal Firewall. The first time you run it, or during an application scan, Norton Personal Firewall identifies pcAnywhere and creates Internet access rules automatically.

For maximum protection, if you run pcAnywhere host, edit the rule to limit its use to only the computers with which you use it. This, coupled with pcAnywhere passwords, provides maximum security.

Using Norton Personal Firewall with a VPN

Norton Personal Firewall works with the following Virtual Private Networks (VPNs):

- Nortel
- VPNRemote
- PGP
- SecureRemote

With most VPNs, when the VPN client is active, you cannot see the Internet or other computers on your local network. You can only see what is available through the VPN server to which you are connected.

CHAPTER 9

Troubleshooting

This section can help you solve many common problems. If you don't find your solution here, you might find a solution elsewhere in this document.

For more information, see "Configuring Norton Personal Firewall for common situations" on page 79.

Troubleshooting Norton Personal Firewall problems

Following are solutions to problems that might occur with Norton Personal Firewall.

What is wrong with this Web site?

Running Norton Personal Firewall can block certain elements of a Web site that prevent it from displaying correctly in your Web browser. In some cases, the site might not display at all.

To see if Norton Personal Firewall is blocking access to the Web site, disable Norton Personal Firewall and try the Web site again. Keep in mind that when you disable Norton Personal Firewall, you are turning off the protection it provides to prevent private information from being sent.

For more information, see "Temporarily disabling Norton Personal Firewall" on page 30.

If you cannot connect with Norton Personal Firewall disabled, there might be a problem with the Internet or your Internet Service Provider.

It could be blocking cookies

Many Web sites require that cookies be enabled on your computer to display correctly. If you have cookie blocking turned on and the Web page appears to be blank, turn off cookie blocking and try the page again.

To stop blocking cookies

1. On the left side of the Norton Personal Firewall window, click **Privacy Control**.
2. Click **Custom Level**.
3. Set **Cookie Blocking** to Medium or None.

If this fixes the problem, consider making site-specific settings to allow cookies from that site.

It could be a firewall rule

A firewall rule might be blocking the Web site. When this happens, you will usually see a message saying that you could not connect. You can view the firewall rules that have been set up and determine if a rule is blocking the site.

It could be ActiveX or Java blocking

Some Web sites display only ActiveX controls or Java applets. If you are blocking them, nothing appears on these sites.

For more information, see "Setting Java and ActiveX Security Levels" on page 64.

If this fixes the problem, consider making site-specific settings to allow ActiveX controls or Java applets from that site.

It could be script blocking

Some Web sites use JavaScript in their navigation controls and in other places. If Norton Personal Firewall is blocking JavaScript or VB Script, it may cause problems with these Web sites.

To stop blocking JavaScript or VB Scripts

1. At the top of the Norton Personal Firewall window, click **Options**.
2. Click **Advanced Options**.
3. On the Web tab, click the **Active Content** tab.
4. In the list of Web sites, do one of the following:
   - Select the Web site that you want to change.
   - Click **(Defaults)** to change all unlisted Web sites.
5. In the Script box, select **Allow All Scripts To Execute**.

Why can't I post information online?

If you are unable to post information to a Web site, it may be because Privacy Control is blocking the information. Check the Confidential Information list on the Privacy window to see if the information you are trying to enter is being blocked.

To check the information on the Personal Information list

1. On the left side of the Norton Personal Firewall window, click **Privacy Control**.
2. Click **Confidential Info**.

   This opens the list of information that Privacy Control blocks from being transferred to the Internet.

Why doesn't Norton Personal Firewall notify me before letting applications access the Internet?

If Automatic Internet Access Control is enabled, Norton Personal Firewall creates rules for applications it recognizes without notifying you. You can disable Automatic Internet Access Control.

For more information, see "Enabling Automatic Internet Access Control" on page 67.

For more information, see "Adjusting the reporting detail" on page 58.

Why doesn't my local network work?

Norton Personal Firewall blocks the use of Microsoft networking to prevent someone from attaching to your computer across the Internet.

To allow the use of your local network, including file and printer sharing, place the computers on your local network in the Trusted zone or unblock access using System-Wide Settings.

For more information, see "Adding computers on your home network to the Trusted zone" on page 70.

For more information, see "Using Norton Personal Firewall on a home network" on page 82.

Why can't I print to a shared printer?

Norton Personal Firewall blocks the use of Microsoft networking to prevent someone from attaching to your computer across the Internet.

To allow the use of your local network, including printer sharing, place the computers on your local network in the Trusted zone.

For more information, see "Adding computers on your home network to the Trusted zone" on page 70.

How can a Web site get my browser information?

The Browser Privacy settings prevent your browser from sending out browser information. However, some diagnostic sites on the Internet might report browser information even though the Browser Privacy settings are blocking the information:

- If you are not blocking Java, ActiveX, or scripts, the site might be using one of these methods to retrieve the information.

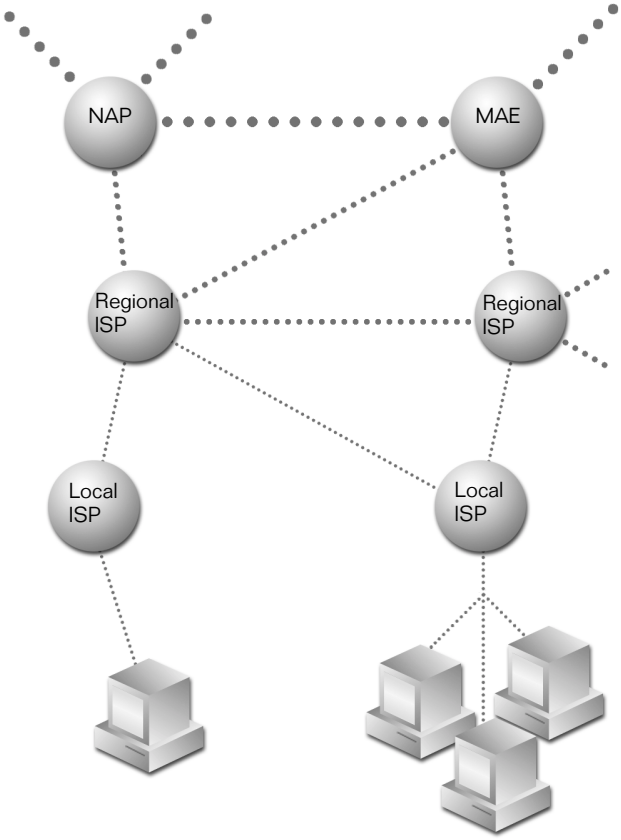
  For more information, see "Setting Java and ActiveX Security Levels" on page 64.

- Sometimes when Web servers do not get the information from the browser, they simply use the last piece of browser information they received instead. You might see the information from the last person who viewed the site.

APPENDIX A

About the Internet

The Internet is the interconnection of millions of computers throughout the world. It comprises the computers and the connections that make it possible for any computer on the Internet to communicate with any other computer on the Internet.



The Internet is analogous to a system of roads and highways. The superhighways of the Internet, called the Internet backbone, carry large amounts of information over long distances. There are interchanges on the backbone, called network access points (NAPs) and metropolitan area exchanges (MAEs). There are regional highways provided by large Internet service providers (ISPs) and local streets provided by local ISPs.

Like a system of roads and highways, the Internet provides multiple routes from one point to another. If one part of the Internet has too much traffic, or is damaged, information is rerouted to take a different route.

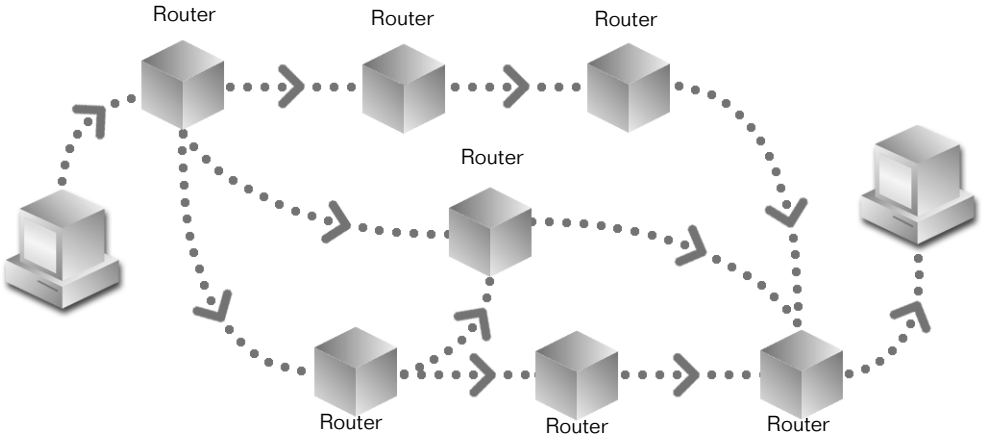
How information is transmitted over the Internet

All information sent across the Internet is communicated using a protocol called TCP/IP. Because all of the computers on the Internet understand this protocol, each one can communicate with every other computer on the Internet. TCP and IP are separate parts of this protocol.

The Internet is a *packet switched network*. Every communication is broken into packets by TCP (Transmission Control Protocol). Each packet contains the address of the sending and receiving computers along with the information to be communicated.

IP (Internet Protocol) is responsible for *routing* the packets to their destinations. Each packet may take a different route across the Internet, and packets may be broken up into *fragments*. Packets travel across the Internet, moving from one *router* to another. Routers look at the

destination address and forward the packet to the next router. IP does not guarantee the delivery of every packet.



On the destination computer, TCP joins the packets into the complete communication. TCP may have to reorder the packets if they are received out of order, and it may have to reassemble fragmented packets. TCP requests retransmission of missing packets.

TCP/IP

TCP/IP is often used to refer to a group of protocols used on the Internet, including UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol), and IGMP (Internet Group Membership Protocol).

UDP

UDP (User Datagram Protocol) is used for functions in which the reliability of TCP is not necessary, such as broadcasting video to multiple computers at once. UDP doesn't provide error correction or retransmission of lost packets.

UDP is secondary in importance to TCP when you browse the Internet.

ICMP

ICMP (Internet Control Message Protocol) packets contain error and control information. They are used to announce network errors, network congestion, timeouts, and to assist in troubleshooting.

Norton Personal Firewall normally allows certain inbound ICMP packets that provide you with information and are a minimal security risk. You can create rules to block some or all ICMP packets.

IGMP

IGMP (Internet Group Membership Protocol) is used to establish memberships in multicast groups. Your computer reports to a nearby router that it wants to receive messages addressed to a specific multicast group.

IGMP does not present a major security risk, but Norton Personal Firewall allows you to block the protocol entirely. This is a good idea if you do not use any applications that require IGMP. If you have problems receiving multicast information, such as movies or PowerPoint presentations, be sure that IGMP is not blocked.

Web information is located on the Internet

Web information is stored as pages, each with a unique name called a URL (Uniform Resource Locator).

When you enter a Web address in the browser address bar or click a link in your Web browser to move to a new Web site, you are giving your browser the URL of the page that you want to view. For example, www.symantec.com is a typical URL.

Each URL maps to the IP address of the computer that stores the Web page. URLs are used because they are easier to remember and type than IP addresses.

Before your browser requests a page, it asks a DNS (Domain Name System) server for the IP address of the Web site. IP addresses are 32-bit numbers expressed as four decimal numbers, each ranging from 0 to 255, and separated by periods: 206.204.104.148. Every computer on the Internet has a unique IP address.

Requesting a page

Once the browser has the IP address, it establishes a TCP *connection* to the Web server and requests the page. Each page that you view requires a new connection with the Web server. In fact, most pages require multiple connections, since each graphic (as well as many other page elements) requires its own connection.

Once a page is loaded, all of the connections are dropped. The process starts over for each page on the site, though your browser does remember the site's IP address.

Some newer Web sites that use HTTP 1.1 (Hypertext Transfer Protocol version 1.1) establish connections that can pass multiple files and stay open for multiple pages with a single connection.

Parts of a URL

A typical URL looks like this: http://www.symantec.com/securitycheck/index.html. Because you might want to block some parts of a domain, while allowing other parts of the same domain, you should understand what comprises a URL.

http://	The *application protocol* used to make the connection. The most common protocol for browsing the Web is http. Your browser assumes this is the application protocol if you don't enter one. Other commonly used protocols include ftp, and gopher.
.com	The *root domain* or *top-level domain*. There are several familiar root domains, including .com, .net, .edu, .org, .mil, and .gov. There are also two-letter root domains for most countries, such as .ca for Canada and .uk for United Kingdom.
symantec.com	The *domain*. This is the domain with which the browser establishes a connection. A domain frequently refers to a single company or organization that might have multiple Web sites on the Internet.
www.symantec.com	The *host*. This is the particular Web site with which the browser communicates. It is also the name for which DNS provides an IP address.

securitycheck	The *folder* or directory that contains the file to be accessed.
index.html	The *file name* of the file to be accessed.

There is one particular URL that identifies your computer to itself, and that is *localhost*. If you have a Web server on your computer, you can type http://localhost and see your Web page. The IP address that corresponds to localhost is 127.0.0.1.

Ports identify applications on a server

Ports, also called *sockets*, provide the location of a particular application or server on the remote computer with which you are trying to establish communication. This makes it possible to run multiple servers on a single computer. For example, many computers on the Internet run both a Web server and an FTP (File Transfer Protocol) server. The Web server uses port 80, while the FTP server uses port 21.

The terms *server* and *service* are used somewhat interchangeably. For example, a Web server provides the HTTP service, while it is usually said that a computer has the *Finger* service running.

Ports are numbered 1 through 65535. Ports 1 through 1023 are known as *well known ports* and are the default ports for many common Internet applications.

Ports are a part of the URL that is rarely seen. The port number follows the host name and a colon. For example:

http://www.symantec.com:80/securitycheck/index.html

Because the most-used ports are standardized, you rarely see port numbers. For example, Web browsers almost always use port 80, so they don't require that you type it unless you need to use a different port.

Well known ports

Some of the most common well known ports are:

Default port	Service name	Application
20	ftp-data	FTP (File Transfer Protocol) data
21	ftp	FTP (File Transfer Protocol) control
23	telnet	Telnet terminal handler
25	smtp	SMTP (Simple Mail Transfer Protocol)
53	domain	DNS (Domain Name Service) lookup
79	finger	Finger
80	http	HTTP (Hypertext Transfer Protocol)
110	pop3	POP3 (Post Office Protocol 3)
113	auth	Ident Authentication Service
119	nntp	NNTP (Network News Transfer Protocol)
137	nbname	NetBIOS name (Microsoft Networking)
138	nbdatagram	NetBIOS datagram (Microsoft Networking)
139	nbsession	NetBIOS session (Microsoft Networking)
143	imap	IMAP (Internet Message Access Protocol)
194	irc	IRC (Internet Relay Chat)
389	ldap	LDAP (Lightweight Directory Access Protocol)
443	https	HTTPS (Secure HTTP)

How computers are identified on the Internet

Millions of computers are connected to the Internet. When you are trying to identify computers, it is easier to work with groups of computers rather than having to identify each one individually. *Subnet masks* provide a way to identify a group of related computers, such as those on your local network.

A typical subnet mask looks like this: 255.255.255.0. At its simplest, each 255 indicates parts of the IP address that are the same for all computers within the subnet, while the 0s indicate parts of the IP address that are different.

Subnet masks are always used in conjunction with a base IP address.

For example:

Base IP address: 10.0.0.1

Subnet mask: 255.255.255.0

In this example, the range of IP addresses that the base IP address and subnet mask identify range from 10.0.0.1 to 10.0.0.255. The most common subnet mask used is 255.255.255.0 because it identifies a relatively small group of IP addresses, up to 254 computers. It is commonly used for very small groups of computers, including groups as small as two computers.

APPENDIX B

Understanding Internet risks

Norton Personal Firewall protects you from the major risks associated with the Internet. Those risks include the threat of hacker attack, malicious code in active content, exposure to inappropriate content, exposure of private information, and getting viruses from infected files.

Risks from hackers

The word *hacker* originally meant someone who could solve computer problems and write computer programs quickly and elegantly. However, the meaning of the term has changed to mean someone who uses his or her computer knowledge for illicit purposes. Since hacker started out as a complimentary term, some people use the word *cracker* for the derogatory form. In this text, hacker is used in its current, non-complimentary meaning.

You might also hear other terms for hackers, including *script-kiddies*, *wannabes*, *packet monkeys* and *cyberpunks*. These are all terms for hackers-in-training that use applications written by others (more advanced hackers) to attack computers on the Internet.

The process of a hacker attack

Most hacker attacks use the following process:

- Information gathering: The hacker gathers as much information about your computer as possible. The hacker attempts to find vulnerabilities without letting you know that your computer is under attack.
- Initial access: The hacker exploits a vulnerability found during information gathering and establishes an entry point into your computer.
- Privilege escalation: The hacker gains access to more of your computer.
- Covering tracks: The hacker hides or removes evidence of the visit, sometimes leaving a doorway open for return.

Information gathering

The first step in information gathering is acquiring a target. A hacker can choose a person or company to attack, or search the Internet for an unprotected target that will be easy to hack. The amount of information available about you on the Internet is directly related to your level of Web presence. If you have a domain name and a Web site, a lot more information is publicly available than would be if you only have an email address.

If a hacker has chosen a specific target, such as a company or organization, many resources on the Internet assist in gathering information. Most of them have legitimate uses, such as InterNic, which provides the Whois database of registered domain names. There are integrated tools, such as Sam Spade, which provides more than 20 different tools for finding and analyzing Internet information.

Using these tools, a hacker can learn a lot about a potential target. Given a domain name, it's easy to use the Whois database to find out the name and address of the owner, as well as the name and phone number of the administrative and technical contacts. While this information usually can't be used directly to attack a network or computer, it can be used to gather more information. It's much easier to call a company, impersonate a network administrator, and ask a user for a password than it is to attack the network.

If a hacker doesn't have a specific target in mind, many tools are available for scanning the Internet and finding possible targets. The simplest scan is a *ping* scan, which can quickly scan thousands of computers. The hacker

uses a program to ping computers at a series of IP addresses. Responses tell the hacker that a computer exists at that IP address. When Norton Personal Firewall is running, your computer is hidden from ping scans because your computer does not respond. The hacker does not learn that there is a computer at your IP address by pinging it.

Port scans are more comprehensive, usually performed on a single computer. A port scan can tell a hacker what services are running, such as HTTP and FTP. Each service that is running provides a potential entry point for the hacker. On unprotected computers, unused ports respond that they are closed, thus telling the hacker that a computer exists at that IP address. Norton Personal Firewall does not respond to scans of unused ports, giving them a *stealth* appearance.

Initial access

The easiest way for a hacker to access a Windows computer is to use Microsoft networking. On many computers, Microsoft networking is enabled so that anyone on the network can connect to it.

Microsoft's NetBIOS networking uses three of the Well Known Ports. These ports are used to establish connections between computers on a Microsoft network. In fact, they normally advertise the name of your computer over the local network. This is what you want on your own network, but it is not what you want on the Internet. Norton Personal Firewall is preset to block these ports and prevent someone on the Internet from connecting to your computer using Microsoft networking. If your computer is connected to a local network as well as to the Internet, you must change some settings to allow communication with the other computers on your network. Norton Personal Firewall still protects you from Internet risks while allowing you to use your local network.

For more information, see "Well known ports" on page 99.

For more information, see "Using Norton Personal Firewall on a home network" on page 82.

Privilege escalation

Once a hacker has connected to your computer, the next step is to gain as much control as possible. The steps involved and the results obtained vary greatly depending on the version of Windows running on the target computer.

On computers running Windows 95, Windows 98, or Windows Me, once a hacker has gained access to the computer, there is no need for escalation. They have full control of the computer. Luckily, these versions of Windows don't have much in the way of remote control features, so they are relatively easy to protect.

On computers running Windows NT or Windows 2000, the hacker will attempt to gain administrative rights to the computer. The key to getting administrative rights is usually a password. Instead of guessing, the hacker can download your password file and crack it.

Another tactic is to place a *Trojan horse* program on your computer. If a hacker can place a program such as Back Orifice, Subseven, or NetBus on your computer and get it running, it is possible to take control of the computer.

Other Trojan horse programs might record all your keystrokes to capture passwords and other sensitive data. Norton Personal Firewall blocks the ports that Remote Access Trojan horse programs use to communicate over the Internet.

Covering tracks

When a hacker has gained as much control of a computer as possible, the task turns to concealing the evidence. As long as you don't know that a hacker has compromised your computer, you won't take steps to stop such actions.

On Windows NT and Windows 2000, hackers will try to turn off auditing and modify or clear the event logs. On any computer, the hacker may hide files so they are available for future visits. In extreme cases, a hacker might format the hard drive of a compromised computer to avoid identification.

Risks from active content

ActiveX controls and Java applets are called *active content* because they can do more than display text or graphics. Most active content is safe. Common uses of active content are pop-up menus and up-to-date stock quotes.

Both ActiveX and Java are supposed to be safe to run in your browser. ActiveX uses a system of digital certificates that lets you decide if you want an ActiveX control to run. Digital certificates appear as dialog boxes that

ask if you want to install and run a control that appears when you are browsing the Web.

There are several problems with this system of using digital certificates. Some controls do not have certificates, and some certificates provide very little information about what the control does.

Java was originally designed to be safe to run in a browser. The Java *sandbox* was designed to prevent Java applets from reaching outside the browser to do anything that might harm your computer. However, hackers and security experts continually find ways to get around Java's safeguards and use Java's features in ways not conceived of by its developers.

Norton Personal Firewall monitors active content and can block all active content or warn you whenever active content is encountered.

Risks to your privacy

The Internet presents several risks to your privacy. Some sites collect and save personal information, such as credit card numbers. Some sites track your Internet usage. Some applications send information about your computer usage to Web sites without your permission.

Sending confidential information

You probably don't want confidential information, such as credit card numbers, or your home phone number, to be sent unencrypted over the Internet. Privacy Control prevents confidential information from being entered on Web sites that do not use secure, encrypted communications, and from being sent on instant messenger programs.

Good cookies and bad cookies

Cookies are messages sent to your browser by a Web site and stored as small files on your computer. They are often used by Web sites to track your visits. In most cases, the cookie file does not contain any personal information, instead carrying only an identifier that identifies you to a Web site.

Good cookies

In their most benign form, cookies last only until you close your browser. This type of cookie is mainly used to help remember choices you have made as you navigate through a Web site.

Many sites leave cookies on your computer so that they recognize you when you return to their site. These cookies identify you so that options you have chosen in the past are used for your current visit to the site. If you frequent a site that remembers the stocks that you want to track, for example, it probably uses this kind of cookie.

Bad cookies

In one of their malevolent forms, cookies from one Web site might track your visits to a different Web site. For example, most of the ads that you see on Web sites do not come directly from the site that you are viewing, but from sites that provide ads to many different sites. When the advertising site displays the ad, it can access cookies on your computer. This allows the advertising company to track your Web usage over a broad range of sites and profile your browsing habits.

Blocking cookies

Norton Personal Firewall can block all cookies or it can notify you of each cookie request. If you block all cookies, you will lose functionality at many Web sites. For example, you might not be able to make purchases from some Internet stores. If you choose to be prompted each time a Web site tries to create a cookie, you can evaluate each request and block those that are not from the site that you are viewing. Norton Personal Firewall can block or allow cookies from particular domains or Web sites.

Tracking Internet use

As you browse the Internet, most browsers freely pass on several bits of information that you might want to keep confidential. One item that your browser normally passes to Web sites is the URL of the page from which you came. This information is used by some Web sites to help you navigate inside the Web site, but it can also be used to identify the Web site you came from. In other words, it can be used to track your Web usage. Norton Personal Firewall blocks this information.

Your browser also sends information about itself and the operating system that you are using. While Norton Personal Firewall can block this information, it is usually used by Web sites to provide Web pages that are appropriate to your browser.

A possibly more sinister invasion of your privacy is found in programs you install on your computer that, without your knowledge, report information back to a Web site. Several programs that help you download and install files have been discovered to report your activities across the Internet. Norton Personal Firewall protects your privacy by alerting you to these communications.

Risks from Trojan horses and viruses

Nowadays, with so many computers connected by networks and the Internet, viruses can spread more rapidly than they could in the days of *sneakernet*, when files were transferred from computer to computer on disks. Additionally, the risk has broadened from viruses to Trojan horses, *worms,* and *zombies*.

A virus is a program or code that replicates by attaching itself to another program, a boot sector, a partition sector, or a document that supports macros. Many viruses just replicate, but others do damage. A virus can arrive in a document that you receive by email.

A Trojan horse is a program that does not replicate, but damages or compromises the security of the computer. Typically, it relies on someone emailing it to you; it does not email itself. A Trojan horse may arrive disguised as useful software. Some Trojan horse programs do malicious things to the computer on which they are run, while others, such as Back Orifice, provide remote control capabilities for hackers.

A worm is a program that makes copies of itself—for example, from one disk drive to another, or by sending itself through email. It may do damage or compromise the security of the computer. A worm can arrive as an attachment to an email that has a subject that tempts you to open it.

A zombie program is a dormant program secretly implanted on a computer. Later, it is awakened to aid in a collective attack on another computer. Zombie programs don't normally damage the computer on which they reside, but are used to attack other computers. A zombie program can arrive as an email attachment.

Norton Personal Firewall ensures that Trojan horse programs do not communicate over the Internet. This means that you are protected from hackers who use Trojan horse programs.

The likelihood of being attacked

The Internet presents many risks. What are the odds that your home computer will be the subject of an attack?

The chance of a hacker singling out your computer from all of those on the Internet is probably very slim. However, the use of these tools by neophyte hackers, or script kiddies, to find targets means that your computer will be scanned relatively frequently for vulnerabilities. The more vulnerabilities found, the more inviting your computer is to the hacker.

The tools that hackers use to find vulnerable targets can scan large groups of computers on the Internet. The hacker simply enters a range of IP addresses to be scanned and clicks OK. The program checks each IP address in the range to see if a computer is there. If it finds a computer, it performs a series of tests to identify vulnerabilities, such as having Microsoft networking enabled over the Internet. The hacker returns to find a list of computers and their vulnerabilities.

Norton Personal Firewall protects you from these scans by making your computer almost invisible. Your computer simply won't respond to the queries that these scanners send. This means that your computer will exhibit no vulnerabilities to the hacker, making it a poor target for attack.

Service and support solutions

Service and support information is available from the Help system of your Symantec product. Click the Service and Support topic in the Help index.

Technical support

Symantec offers several technical support options:

- Online Service and Support

  Connect to the Symantec Service & Support Web site at http://service.symantec.com, select your user type, and then select your product and version. This gives you access to current hot topics, knowledge bases, file download pages, multimedia tutorials, contact options, and more.

- PriorityCare telephone support

  PriorityCare fee-based telephone support services are available to all registered customers. For complete information, please call our automated fax retrieval service at (800) 554-4403 and request document 933000.

  You can also access the PriorityCare number for your product through the Service & Support Web site. You'll be led through the online options first, and then to the telephone contact options available for your product and version.

- Automated fax retrieval

  Use your fax machine to receive general product information, fact sheets, and product upgrade order forms by calling (800) 554-4403. For technical application notes, call (541) 984-2490.

Support for old and discontinued versions

When a new version of this software is released, registered users will receive upgrade information in the mail. Telephone support will be provided for the old version for up to twelve months after the release of the new version. Technical information may still be available through the Service & Support Web site (http://service.symantec.com).

When Symantec announces that a product will no longer be marketed or sold, telephone support will be discontinued 60 days later. Support will be available for discontinued products from the Service & Support Web site only.

Customer service

Access customer service options through the Service & Support Web site at http://service.symantec.com. From this site, you can receive assistance with non-technical questions, and for information on how to do the following:

- Subscribe to the Symantec Support Solution of your choice.
- Obtain product literature or trialware.
- Locate resellers and consultants in your area.
- Replace missing or defective CD-ROMS, disks, manuals, and so on.
- Update your product registration with address or name changes.
- Get order, return, or rebate status information.
- Access customer service FAQs.
- Post a question to a Customer Service representative.

For upgrade orders, visit the online upgrade center at:
http://www.symantecstore.com

Worldwide service and support

Technical support and customer service solutions vary by country. For information on Symantec and International Partner locations outside of the United States, please contact one of the service and support offices listed below, or connect to http://service.symantec.com and select your region under the Global Service and Support.

Service and support offices

North America

Symantec Corporation
175 W. Broadway
Eugene, OR 97401
U.S.A.

http://www.symantec.com/
Fax: (541) 984-8020

Automated Fax Retrieval

(800) 554-4403
(541) 984-2490

Argentina and Uruguay

Symantec Region Sur
Cerrito 1054 - Piso 9
1010 Buenos Aires
Argentina

http://www.service.symantec.com/mx
+54 (11) 5382-3802

Asia/Pacific Rim

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Sydney
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 8879-1000
Fax: +61 (2) 8879-1001

Brazil

Symantec Brasil
Market Place Tower
Av. Dr. Chucri Zaidan, 920
12° andar
São Paulo - SP
CEP: 04583-904
Brasil, SA

http://www.service.symantec.com/br
+55 (11) 5189-6300
Fax: +55 (11) 5189-6210

Europe, Middle East, and Africa

Symantec Customer Service Center
P.O. Box 5689
Dublin 15
Ireland

http://www.symantec.com/region/reg_eu/
+353 (1) 811 8032

Mexico

Symantec Mexico
Blvd Adolfo Ruiz Cortines,
No. 3642 Piso 14
Col. Jardines del Pedregal
Ciudad de México, D.F.
C.P. 01900
México

http://www.service.symantec.com/mx
+52 (5) 661-6120

Other Latin America

Symantec Corporation
9100 South Dadeland Blvd.
Suite 1810
Miami, FL 33156
U.S.A.

http://www.service.symantec.com/mx

Subscription policy

If your Symantec product includes virus, firewall, or web content protection, you might be entitled to receive protection updates via LiveUpdate. The length of the subscription could vary by Symantec product.

When you near the end of your subscription, you will be prompted to subscribe when you start LiveUpdate. Simply follow the instructions on the screen. After your initial subscription ends, you must renew your subscription before you can update your virus, firewall, or web content protection. Without these updates, your vulnerability to attack increases. Renewal subscriptions are available for a nominal charge.

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

July 13, 2001

Norton™ Personal Firewall
CD Replacement Form

CD REPLACEMENT: After your 60-Day Limited Warranty, if your CD becomes unusable, fill out and return 1) this form, 2) your damaged CD, and 3) your payment (see pricing below, add sales tax if applicable), to the address below to receive replacement CD. *DURING THE 60-DAY LIMITED WARRANTY PERIOD, THIS SERVICE IS FREE.* You must be a registered customer in order to receive CD replacements.

FOR CD REPLACEMENT

Please send me: ___ CD Replacement

Name _____

Company Name _____

Street Address (No P.O. Boxes, Please)_____

City _____ State _____ Zip/Postal Code _____

Country* _____Daytime Phone _____

Software Purchase Date _____

*This offer limited to U.S., Canada, and Mexico. Outside North America, contact your local Symantec office or distributer.

Briefly describe the problem:_____

_____

CD Replacement Price	$ 10.00
Sales Tax (See Table)	_____
Shipping & Handling	$ 9.95
TOTAL DUE	_____

SALES TAX TABLE: AZ (5%), CA (7.25%), CO (3%), CT (6%), DC (5.75%), FL (6%), GA (4%), IA (5%), IL (6.25%), IN (5%), KS (4.9%), LA (4%), MA (5%), MD (5%), ME (6%), MI (6%), MN (6.5%), MO (4.225%), NC (6%), NJ (6%), NY (4%), OH (5%), OK (4.5%), PA (6%), SC (5%), TN (6%), TX (6.25%), VA (4.5%), WA (6.5%), WI (5%). Please add local sales tax (as well as state sales tax) in AZ, CA, FL, GA, MO, NY, OH, OK, SC, TN, TX, WA, WI.

FORM OF PAYMENT ** (CHECK ONE):

___ Check (Payable to Symantec) Amount Enclosed $ _____ __ Visa __ Mastercard __ American Express

Credit Card Number _____Expires _____

Name on Card (please print) _____ Signature _____

****U.S. Dollars. Payment must be made in U.S. dollars drawn on a U.S. bank.**

MAIL YOUR CD REPLACEMENT ORDER TO:

Symantec Corporation
Attention: Order Processing
175 West Broadway
Eugene, OR 97401-3003 (800) 441-7234

Please allow 2-3 weeks for delivery within the U.S.

Symantec and Norton are trademarks of Symantec Corporation.
Other brands and products are trademarks of their respective holder/s.
© 2001 Symantec Corporation. All rights reserved. Printed in the U.S.A.

symantec™

I N D E X

A

active content 104
    See also ActiveX controls; Java applets
ActiveX controls 14, 54, 64, 90, 104
Alert Tracker, defined 40
alerts
    ActiveX 54
    Confidential Information 56
    cookie 55
    Internet Access Control 52, 67
    Intrusion Protection 72
    Java 54
    overview 49
    Personal Firewall 65
    Security 50
AOL 32
Application Control configuration 38
applications, accessing Internet. *See* Internet-enabled applications
attacks 72-74, 102-104, 108
AutoBlock 50, 72

B

blocking
    ActiveX controls 54
    browser information 92
    computers 72
    confidential information 15, 44-45, 57, 91, 105
    cookies 46, 56, 90, 105
    email addresses 47
    Internet-enabled applications 53
    Java applets 54
    programs. *See* Internet-enabled applications
broadband connections 79-80, 83
browser
    information 92
    privacy 47

C

cable modem connections 79-80, 83
Changing 46
CompuServe 32
computers
    adding to zones 70
    blocking 72
    names 75
    requirements 17
    specifying 74-76
confidential information 15, 44-46, 56, 91, 105
cookies 15, 46, 55, 78, 90, 105
corporate firewalls 83
credit card numbers 45

D

desktop icon 29
DHCP (Dynamic Host Configuration Protocol) servers 87
dialup connections 79
disabling temporarily, Norton Personal Firewall 30-31
DNS (Domain Name System) 96
DSL connections 79-80, 83
Dynamic Host Configuration Protocol (DHCP) servers 87

E

email 16
encryption 47

F

feature summary 13-16
file sharing 82, 84

firewall rules
for FTP servers 87
problems 90
system-wide 69
for Web servers 86
firewalls
See also Personal Firewall
corporate 83
overview 13
FTP servers 87

G

games 81

H

hackers 101-104
Help 15, 33-34
home networks 82, 92

I

ICMP (Internet Control Message Protocol) 95
icon in notification area 29
IGMP (Internet Group Membership Protocol) 95
Information Wizard
features 24
how to use 24
when it appears 24
information, confidential 15, 44-46, 56, 91, 105
Internet Access Control 65-68, 91
alerts 52
Internet activity information 40
Internet Connection Sharing 83
Internet Control Message Protocol (ICMP) 95
Internet Group Membership Protocol (IGMP) 95
Internet Zone Control 69-71
configuration 39
Internet, overview 93-95, 96
Internet-enabled applications 52, 67
Intrusion Protection 72-74
intrusion protection service 32
IP addresses 75

J

Java applets 14, 54, 64, 90, 104
JavaScript 90

L

LiveUpdate 31
localhost 98

M

messages, viewing 57
multiplayer games 81

N

NetBIOS 80
networks 82, 92
Norton Personal Firewall. *See* Personal Firewall
Norton Privacy Control. *See* Privacy Control
Norton SystemWorks, installing with 26
notification area icon 29

O

online Help 15, 33-34
operating systems 17

P

pcAnywhere 88
Personal Firewall
alerts 65
configuration 35
overview 13, 61
security settings 62-64
status 78
ping scans 102
ports 98-99
hiding 65
scanning 80, 103
printers, sharing 82, 84, 92
privacy
levels 44
risks 105-107
settings 45

Privacy Control 15, 43-47, 91, 105
configuration 36
status 78
problems
browser information 92
network 92
posting information to Web sites 91
printing 92
Web site display 89-91
Prodigy Internet connection 32
product serial number 23
programs, accessing Internet. *See* Internet-enabled applications
proxy servers 84

R

Readme file 34
registering your software 23
removing, Norton Personal Firewall from your computer 26
reporting detail 59
required computer configuration 17
risks
from active content 104
from hackers 101-104
to privacy 105-107
from Trojan horses 107
from viruses 107
routers 83

S

scanning
for Internet-enabled applications 67
ports 80, 103
scripts 90
secure Web sites 47
security
attacks 72-74, 102-104, 108
levels 62-64
Security Alerts 50
Security Assistant 15
after installation 25
Alert Tracker pane 40
Application Control pane 38
Internet Status pane 40
Internet Zone Control pane 39
LiveUpdate pane 40
navigating 35
opening 35
Personal Firewall pane 35
Privacy Control pane 36
serial number 23
Service and Support 109
settings
Personal Firewall 62-64
privacy 45
sharing files and printers 82, 84, 92
sockets 98
starting Norton Personal Firewall 29
status
Personal Firewall 78
Privacy Control 78
stealth ports 65, 103
subnet masks 76, 100
system tray icon 29

T

TCP/IP 94-96
Technical Support 109
Trojan horse programs 107
Trusted zone 70

U

UDP (User Datagram Protocol) 95
Uniform Resource Locator (URL) 75, 96, 97
uninstalling
Norton Personal Firewall 26
other firewall programs 18
previous copies of Norton Personal Firewall 18
URL (Uniform Resource Locator) 75, 96, 97
User Datagram Protocol (UDP) 95

V

VB Script 90
virtual private network (VPN) 88
viruses, risks from 107
VPN (virtual private network) 88

W

Web servers 86
Web sites, display problems 89-91
What's This? Help 33
Windows operating systems 17
worms 107

Z

zombies 107
zones 69-71